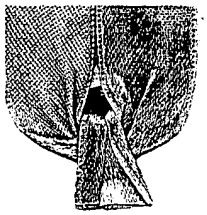


日　本　国　特　許　庁
JAPAN PATENT OFFICE

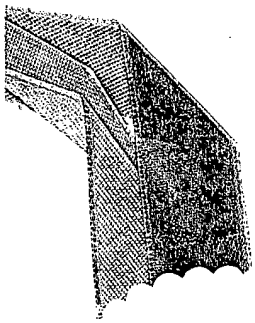
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

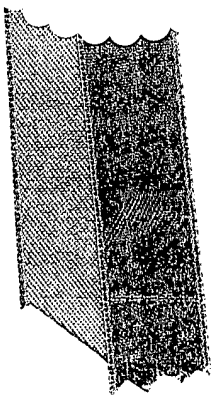
出願年月日
Date of Application: ２０００年１２月１３日

出願番号
Application Number: 特願２０００－３７８２６１

出願人
Applicant(s): ソニー株式会社



CERTIFIED COPY OF
PRIORITY DOCUMENT



２００１年１１月１６日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３０９９７０２

【書類名】　特許願
【整理番号】　0000776311
【提出日】　平成12年12月13日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/60
G09C 1/00
G06K 5/00
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　飯野　陽一郎
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代表者】　出井　伸之
【代理人】
【識別番号】　100082131
【弁理士】
【氏名又は名称】　稲本　義雄
【電話番号】　03-3369-6479
【手数料の表示】
【予納台帳番号】　032089
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9708842
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報記録媒体、情報処理装置および情報処理方法、プログラム記録媒体、並びに情報処理システム

【特許請求の範囲】

【請求項１】　それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報と

が記録されている

ことを特徴とする情報記録媒体。

【請求項２】　前記有効性データと被証明情報とは、電子的なチケットである電子チケットを構成する

ことを特徴とする請求項１に記載の情報記録媒体。

【請求項３】　前記被証明情報は、前記電子チケットの権利内容を、さらに含む

ことを特徴とする請求項２に記載の情報記録媒体。

【請求項４】　前記被証明情報は、その改竄を行うことができないように処理されている

ことを特徴とする請求項３に記載の情報記録媒体。

【請求項５】　前記被証明情報には、電子署名が含められることにより、その改竄を行うことができないように処理されている

ことを特徴とする請求項４に記載の情報記録媒体。

【請求項６】　前記有効性データは、前記電子チケットの使用回数をさらに含む

ことを特徴とする請求項３に記載の情報記録媒体。

【請求項７】　前記有効性データは、暗号化されている

ことを特徴とする請求項１に記載の情報記録媒体。

【請求項８】　前記有効性データは、所定の鍵で暗号化され、

前記所定の鍵は、別の鍵で暗号化されている

ことを特徴とする請求項７に記載の情報記録媒体。

【請求項９】　前記秘密情報は、公開鍵暗号化方式の秘密鍵であり、

前記検証用パラメータは、前記秘密鍵に対応する公開鍵である

ことを特徴とする請求項２に記載の情報記録媒体。

【請求項１０】　前記被証明情報は、前記電子チケットの発行者を識別するための発行者識別情報、前記発行者を検証するための公開鍵、および前記発行者識別情報と公開鍵に対して、所定の認証センタが生成した電子署名からなる、前記発行者の証明書である発行者証明書をさらに含む

ことを特徴とする請求項２に記載の情報記録媒体。

【請求項１１】　それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成手段と、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成手段と、

前記検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成手段と、

前記有効性データと被証明情報とからなる情報セットを外部に出力する出力手段と

を備えることを特徴とする情報処理装置。

【請求項１２】　前記有効性データと被証明情報とからなる情報セットは、電子的なチケットである電子チケットを構成する

ことを特徴とする請求項１１に記載の情報処理装置。

【請求項１３】　前記被証明情報生成手段は、前記電子チケットの権利内容をさらに含む前記被証明情報を生成する

ことを特徴とする請求項１２に記載の情報処理装置。

【請求項１４】　前記被証明情報生成手段は、前記被証明情報を、その改竄を行うことができないように処理する

ことを特徴とする請求項１３に記載の情報処理装置。

【請求項１５】　前記被証明情報生成手段は、前記被証明情報に、電子署名を含めることにより、その改竄を行うことができないように処理する

ことを特徴とする請求項１４に記載の情報処理装置。

【請求項１６】　前記出力手段は、前記電子チケットの情報としての前記有効性データおよび被証明情報を外部に出力する際に、出力相手の装置との間で認証処理を行う

ことを特徴とする請求項１２に記載の情報処理装置。

【請求項１７】　前記出力手段は、前記有効性データを暗号化して出力する

ことを特徴とする請求項１２に記載の情報処理装置。

【請求項１８】　前記出力手段は、

公開鍵暗号化方式の公開鍵、およびその公開鍵に対して、所定の認証センタが生成した電子署名からなる、正当な装置であることを証明する装置証明書を、相手の装置に送信し、

前記相手の装置から送信されてくる暗号鍵であって、前記装置証明書に含まれる前記公開鍵で暗号化されたものを、前記公開鍵に対応する秘密鍵で復号し、

前記暗号鍵で、前記有効性データを暗号化する

ことを特徴とする請求項１７に記載の情報処理装置。

【請求項１９】　前記有効性データ生成手段は、公開鍵暗号化方式の秘密鍵を、前記秘密情報としてを含む有効性データを生成し、

前記検証用パラメータ生成手段は、前記秘密鍵に対応する公開鍵を、前記検証用パラメータとして生成する

ことを特徴とする請求項１２に記載の情報処理装置。

【請求項２０】　前記被証明情報生成手段は、前記電子チケットの発行者を識別するための発行者識別情報、前記発行者を検証するための公開鍵、および前記発行者識別情報と公開鍵に対して、所定の認証センタが生成した電子署名からなる、前記発行者の証明書である発行者証明書をさらに含む前記被証明情報を生成する

ことを特徴とする請求項１２に記載の情報処理装置。

【請求項２１】　それ自体を外部に示すことなく、それが存在することを証

明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成ステップと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成ステップと、

前記検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成ステップと、

前記有効性データと被証明情報とからなる情報セットを外部に出力する出力ステップと

を備えることを特徴とする情報処理方法。

【請求項２２】　コンピュータに実行させるプログラムが記録されているプログラム記録媒体において、

それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成ステップと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成ステップと、

前記検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成ステップと、

前記有効性データと被証明情報とからなる情報セットを外部に出力する出力ステップと

を備えるプログラムが記録されている

ことを特徴とするプログラム記録媒体。

【請求項２３】　それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報と

からなる情報セットを処理する情報処理装置において、

前記情報セットを記憶する記憶手段と、

前記被証明情報を、その被証明情報を検査する検査装置に送信する被証明情報送信手段と、

前記秘密情報の存在を証明する証明データを生成し、前記検査装置に送信する証明データ生成手段と

を備えることを特徴とする情報処理装置。

【請求項２４】　前記有効性データと被証明情報とからなる情報セットは、電子的なチケットである電子チケットを構成する

ことを特徴とする請求項２３に記載の情報処理装置。

【請求項２５】　前記有効性データを、第１の暗号鍵で暗号化する第１の暗号化手段と、

前記第１の暗号鍵で暗号化された前記有効性データを、前記第１の鍵で復号する第１の復号手段と

をさらに備え、

前記記憶手段は、前記第１の暗号鍵で暗号化された前記有効性データを記憶する

ことを特徴とする請求項２３に記載の情報処理装置。

【請求項２６】　前記第１の暗号鍵は、所定のタイミングで更新される

ことを特徴とする請求項２５に記載の情報処理装置。

【請求項２７】　前記第１の暗号鍵を、第２の暗号鍵で暗号化する第２の暗号化手段と、

前記第２の鍵で暗号化された前記第１の暗号鍵を、前記第２の暗号鍵で復号する第２の復号手段と

をさらに備え、

前記記憶手段は、前記第２の鍵で暗号化された前記第１の暗号鍵も記憶する

ことを特徴とする請求項２５に記載の情報処理装置。

【請求項２８】　前記第２の暗号鍵は、前記第２の暗号化手段および復号手段を構成するハードウェアに内蔵される

ことを特徴とする請求項２７に記載の情報処理装置。

【請求項２９】　前記第２の暗号鍵は、所定のタイミングで更新される

ことを特徴とする請求項２７に記載の情報処理装置。

【請求項３０】　前記被証明情報は、前記電子チケットの権利内容をさらに含む

ことを特徴とする請求項２４に記載の情報処理装置。

【請求項３１】　前記被証明情報は、その改竄を行うことができないように処理されている

ことを特徴とする請求項２４に記載の情報処理装置。

【請求項３２】　前記被証明情報は、電子署名が含められることにより、その改竄を行うことができないように処理されている

ことを特徴とする請求項３１に記載の情報処理装置。

【請求項３３】　前記秘密情報は、公開鍵暗号化方式の秘密鍵であり、

前記検証用パラメータは、前記秘密鍵に対応する公開鍵であり、

前記証明データ生成手段は、前記秘密鍵を用いた処理を行うことによって、前記証明データを生成する

ことを特徴とする請求項２４に記載の情報処理装置。

【請求項３４】　前記有効性データは、前記電子チケットの使用回数を含み、　前記証明データ生成手段は、所定の情報と前記使用回数を、前記秘密鍵を用いて処理し、その処理結果と前記使用回数を送信する

ことを特徴とする請求項３３に記載の情報処理装置。

【請求項３５】　前記証明データ生成手段により前記使用回数が送信されるごとに、前記記憶手段に記憶された前記有効性データに含まれる使用回数をインクリメントするインクリメント手段をさらに備える

ことを特徴とする請求項３４に記載の情報処理装置。

【請求項３６】　前記記憶手段に記憶された前記有効性データおよび被証明情報からなる電子チケットの情報を、他の装置に譲渡する譲渡手段をさらに備える

ことを特徴とする請求項２４に記載の情報処理装置。

【請求項３７】　前記電子チケットの情報を譲渡する際に、前記他の装置との間で認証処理を行う認証手段をさらに備える

ことを特徴とする請求項３６に記載の情報処理装置。

【請求項３８】　前記譲渡手段は、前記有効性データを暗号化して、前記他の装置に送信する

ことを特徴とする請求項３６に記載の情報処理装置。

【請求項３９】　前記譲渡手段は、

公開鍵暗号化方式の公開鍵、およびその公開鍵に対して、所定の認証センタが生成した電子署名からなる、正当な装置であることを証明する装置証明書を、前記他の装置に送信し、

前記相手の装置から送信されてくる暗号鍵であって、前記装置証明書に含まれる前記公開鍵で暗号化されたものを、前記公開鍵に対応する秘密鍵で復号し、

前記暗号鍵で、前記有効性データを暗号化する

ことを特徴とする請求項３８に記載の情報処理装置。

【請求項４０】　前記譲渡手段は、前記電子チケットの情報を、他の装置に譲渡するとともに、その電子チケットの情報を、前記記憶手段から削除する

ことを特徴とする請求項３６に記載の情報処理装置。

【請求項４１】　前記有効性データおよび被証明情報からなる電子チケットの情報を、他の装置から譲受する譲受手段をさらに備える

ことを特徴とする請求項２４に記載の情報処理装置。

【請求項４２】　前記電子チケットの情報を譲受する際に、前記他の装置との間で認証処理を行う認証手段をさらに備える

ことを特徴とする請求項４１に記載の情報処理装置。

【請求項４３】　前記譲受手段は、前記他の装置からの電子チケットの情報を構成する被証明情報の正当性を確認する

ことを特徴とする請求項４２に記載の情報処理装置。

【請求項４４】　前記被証明情報は、前記電子チケットの発行者を識別するための発行者識別情報、前記発行者を検証するための公開鍵、および前記発行者識別情報と公開鍵に対して、所定の認証センタが生成した電子署名からなる、前記発行者の証明書である発行者証明書をさらに含み、

前記譲受手段は、前記発行者証明書に基づいて、前記被証明情報の正当性を確

認する

ことを特徴とする請求項４３に記載の情報処理装置。

【請求項４５】　前記被証明情報には、電子署名が含まれており、

前記譲受手段は、前記電子署名に基づいて、前記被証明情報の正当性を確認する

ことを特徴とする請求項４３に記載の情報処理装置。

【請求項４６】　前記被証明情報には、前記公開鍵に対応する秘密鍵によって生成された電子署名が付加されており、

前記譲受手段は、前記電子署名を、前記公開鍵で処理することにより、前記被証明情報の正当性を確認する

ことを特徴とする請求項４４に記載の情報処理装置。

【請求項４７】　前記譲受手段は、暗号化されている前記有効性データを受信する

ことを特徴とする請求項４１に記載の情報処理装置。

【請求項４８】　前記譲受手段は、

公開鍵暗号化方式の公開鍵、およびその公開鍵に対して、所定の認証センタが生成した電子署名からなる、正当な装置であることを証明する装置証明書を、前記他の装置から受信し、

所定の暗号鍵を、前記装置証明書に含まれる前記公開鍵で暗号化したものを、前記他の装置に送信し、

前記所定の暗号鍵で暗号化された前記有効性データを受信する

ことを特徴とする請求項４７に記載の情報処理装置。

【請求項４９】　それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報と

からなる情報セットを処理する情報処理方法において、

前記被証明情報を、その被証明情報を検査する検査装置に送信する被証明情報

送信ステップと、

前記秘密情報の存在を証明する証明データを生成し、前記検査装置に送信する証明データ生成ステップと

を備えることを特徴とする情報処理方法。

【請求項５０】　それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報と

からなる情報セットを、コンピュータに処理させるプログラムが記録されているプログラム記録媒体において、

前記被証明情報を、その被証明情報を検査する検査装置に送信する被証明情報送信ステップと、

前記秘密情報の存在を証明する証明データを生成し、前記検査装置に送信する証明データ生成ステップと

を備えるプログラムが記録されている

ことを特徴とするプログラム記録媒体。

【請求項５１】　それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報と

からなる情報セットを検査する情報処理装置において、

他の装置からの前記被証明情報を受信する被証明情報受信手段と、

前記他の装置からの前記秘密情報の存在を証明する証明データを受信する証明データ受信手段と、

前記証明データと、前記被証明情報に含まれる検証用パラメータとを用いて、前記他の装置における前記秘密情報の存否を判定する存否判定手段と

を備えることを特徴とする情報処理装置。

【請求項５２】　前記有効性データと被証明情報とからなる情報セットは、電子的なチケットである電子チケットを構成する

ことを特徴とする請求項５１に記載の情報処理装置。

【請求項５３】　前記被証明情報は、前記電子チケットの権利内容を、さらに含み、

前記権利内容が、所定のサービス提供の条件を満たすかどうかを判定する権利内容判定手段をさらに備える

ことを特徴とする請求項５２に記載の情報処理装置。

【請求項５４】　前記秘密情報は、公開鍵暗号化方式の秘密鍵であり、

前記検証用パラメータは、前記秘密鍵に対応する公開鍵であり、

前記証明データは、前記有効性データに含まれる前記秘密鍵を用いた処理を行うことにより生成されたものであり、

前記存否判定手段は、前記証明データを、前記公開鍵で処理することにより、前記秘密情報の存否を判定する

ことを特徴とする請求項５２に記載の情報処理装置。

【請求項５５】　前記有効性データは、前記電子チケットの使用回数を含み、　前記証明データは、所定の情報と前記使用回数を、前記秘密鍵を用いて処理した処理結果と、前記使用回数とで構成される

ことを特徴とする請求項５４に記載の情報処理装置。

【請求項５６】　前記他の装置からの電子チケットの情報を構成する被証明情報の正当性を確認する確認手段をさらに備える

ことを特徴とする請求項５２に記載の情報処理装置。

【請求項５７】　前記被証明情報は、前記電子チケットの発行者を識別するための発行者識別情報、前記発行者を検証するための公開鍵、および前記発行者識別情報と公開鍵に対して、所定の認証センタが生成した電子署名からなる、前記発行者の証明書である発行者証明書をさらに含み、

前記確認手段は、前記発行者証明書に基づいて、前記被証明情報の正当性を確認する

ことを特徴とする請求項５６に記載の情報処理装置。

【請求項５８】　前記被証明情報には、電子署名が含められており、

前記確認手段は、前記電子署名に基づいて、前記被証明情報の正当性を確認する

ことを特徴とする請求項５６に記載の情報処理装置。

【請求項５９】　前記被証明情報には、前記公開鍵に対応する秘密鍵によって生成された電子署名が含められており、

前記確認手段は、前記電子署名を、前記公開鍵で処理することにより、前記被証明情報の正当性を確認する

ことを特徴とする請求項５７に記載の情報処理装置。

【請求項６０】　それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報と

からなる情報セットを検査する情報処理方法において、

他の装置からの前記被証明情報を受信する被証明情報受信ステップと、

前記他の装置からの前記秘密情報の存在を証明する証明データを受信する証明データ受信ステップと、

前記証明データと、前記被証明情報に含まれる検証用パラメータとを用いて、前記他の装置における前記秘密情報の存否を判定する存否判定ステップと

を備えることを特徴とする情報処理方法。

【請求項６１】　それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報と

からなる情報セットを検査する処理を、コンピュータに行わせるプログラムが記録されているプログラム記録媒体において、

他の装置からの前記被証明情報を受信する被証明情報受信ステップと、

前記他の装置からの前記秘密情報の存在を証明する証明データを受信する証明データ受信ステップと、

前記証明データと、前記被証明情報に含まれる検証用パラメータとを用いて、前記他の装置における前記秘密情報の存否を判定する存否判定ステップと

を備えるプログラムが記録されている

ことを特徴とするプログラム記録媒体。

【請求項６２】　第１乃至第３の情報処理装置から構成される情報処理システムにおいて、

前記第１の情報処理装置は、

それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成手段と、

前記秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成手段と、

前記検証用パラメータを含み、前記有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成手段と、

前記有効性データと被証明情報とからなる情報セットを外部に出力する出力手段と

を備え、

前記第２の情報処理装置は、

前記情報セットを記憶する記憶手段と、

前記被証明情報を、その被証明情報を検査する前記第３の情報処理装置に送信する被証明情報送信手段と、

前記秘密情報の存在を証明する証明データを生成し、前記第３の情報処理装置に送信する証明データ生成手段と

を備え、

前記第３の情報処理装置は、

前記第２の情報処理装置からの前記被証明情報を受信する被証明情報受信手段と、

前記第２の情報処理装置からの前記秘密情報の存在を証明する証明データを受信する証明データ受信手段と、

前記証明データと、前記被証明情報に含まれる検証用パラメータとを用いて、前記第２の情報処理装置における前記秘密情報の存否を判定する存否判定手段とを備える

ことを特徴とする情報処理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報記録媒体、情報処理装置および情報処理方法、プログラム記録媒体、並びに情報処理システムに関し、特に、例えば、利便性の高い電子チケットを実現することができるようにする情報記録媒体、情報処理装置および情報処理方法、プログラム記録媒体、並びに情報処理システムに関する。

【０００２】

【従来の技術】

例えば、乗車券、入場券、予約券、会員書、許可書、サービス券などは、それを所持する者が、そこに記されている権利を有することを証明する。

【０００３】

いま、このように、それを所持する者が有する権利を証明するものを、チケットと呼ぶこととすると、紙（紙に類するプラスチック等も含む）によるチケットは、携帯に便利な大きさの紙等に、所定事項を印刷することで実現されることから、携帯に便利であるという「携帯性」を有する。

【０００４】

また、紙によるチケットを、単なる印刷を行って実現した場合には、偽造等を防止することが困難である。そこで、従来より、偽造等を防止するための手段として、例えば、特殊な印刷や、検印、あるいは透かしが付された紙などが用いられている。従って、紙によるチケットは、正当な発行者のみが発行でき、容易には偽造できないという「複製防止機能」を有する。

【０００５】

さらに、紙によるチケットは、それを所持するものが有する権利を証明する「権利証明機能」や、チケット自体を譲渡することで、第三者に、そのチケットに基づく権利を容易に譲渡することができるという「譲渡性」を有する。

【０００６】

ところで、従来より、電話網やコンピュータネットワークを経由してチケットの取得の予約手続きを行うことが可能であったが、チケットの最終的な受け取りは、郵送あるいは手渡しによって行われており、従って、ユーザは、チケットの受け取りのために、店舗に出向く等の必要があった。

【０００７】

そこで、最近では、コンピュータネットワーク技術の進歩に伴い、チケットを電子情報化し、チケット自体を通信回線を介してやり取りする電子チケットシステムの研究、開発が行われている。いま、このように電子情報化されたチケットを、電子チケットと呼ぶこととすると、電子チケットによれば、ユーザは、その受け取りのために、店舗等に出向く必要がなくなり、さらには、チケットの流通コストおよび管理コストを削減すること等が可能となる。

【０００８】

電子チケットシステムを実現する方法としては、例えば、特開平8-147500号公報等に開示されているような第１の方法や、特開平11-31204号公報等に開示されているような第２の方法が提案されている。

【０００９】

即ち、第１の方法では、電子チケットの実体である電子チケット情報が複製されることにより、電子チケットに基づく権利を多重利用（行使）することができないように、電子チケット情報が、耐タンパー(tamper)性のあるハードウェアによって保持される。

【００１０】

そして、電子チケットによってサービスの提供を受ける場合等においては、その電子チケット情報を保持している保持装置と、その電子チケット情報を検査する検査装置との間で、お互いが、電子チケットシステムの正当な参加機器であることを確認する認証が、例えば、検査装置が保持装置に対して特別の命令を送り

、暗号化の技術等を用いることによって行われる。この認証によって、保持装置と検査装置とが、互いに正当な機器であることが確認されると、保持装置から検査装置に対して、保持装置が記憶している電子チケット情報が送信される。

【００１１】

以上のように、第１の方法では、電子チケット情報をやりとりする保持装置と検査装置とが、正当な機器であることを確認することによって、正当な機器以外の機器に、電子チケット情報が、不正に漏洩することを防止するようになっている。

【００１２】

従って、第１の方法によれば、電子チケットに基づく権利を有していることの証明、即ち、権利証明を行うために、相手が正当な機器であるかどうかを確認しなければならず、紙によるチケットに比較して不便である。

【００１３】

即ち、紙によるチケットであれば、そのチケットを相手に提示することによって、容易かつ安全に、つまり、相手が誰であるかを確認せずに、かつ、チケットに基づく権利が不正に取得されることを心配することなく、権利証明を行うことができる。しかしながら、第１の方法では、相手を確認し、しかも、権利を証明する電子チケット情報を相手に渡さないと、権利証明を行うことができない。

【００１４】

そこで、第２の方法では、電子チケット情報自体をやりとりするのではなく、電子チケット情報を用いて、所定の処理を行い、その処理結果をやりとりすることによって、権利証明を行うことが可能となっている。

【００１５】

即ち、第２の方法では、認証方法として用いられることが多い、いわゆるチャレンジアンドレスポンス(Challenge & Response)の手法を利用して、権利証明が行われる。

【００１６】

具体的には、まず、電子チケットを検査する検査装置が、乱数を発生し、電子チケット情報を保持する保持装置に送信する。保持装置は、検査装置からの乱数

を受信し、その乱数を、電子チケット情報に含まれる秘密の情報を用いて処理し、その処理結果を、検査装置に送信する。検査装置は、保持装置からの処理結果を、公開された情報を用いて処理し、その処理結果と、保持装置に送信した乱数とに基づいて、電子チケットが正当なものであるかどうかを確認（検査）する。

【００１７】

このようなチャレンジアンドレスポンスは、例えば、いわゆる電子署名を用いて行われ、この場合、電子チケット情報に含まれる秘密の情報は、公開鍵暗号化方式の秘密鍵となり、また、検査装置で用いられる公開された情報は、その秘密鍵に対応する公開鍵となる。そして、保持装置では、検査装置からの乱数（チャレンジ）を、秘密鍵を用いて処理することで、電子署名が作成され、検査装置では、その電子署名（レスポンス）を、公開鍵を用いて処理することにより、その電子署名と、元の乱数との対応が検証される。

【００１８】

以上のような第２の方法によれば、電子チケット情報に含まれる秘密の情報としての秘密鍵は、保持装置の外部に示される公開された情報としての公開鍵から認識することはできず、さらに、チャレンジアンドレスポンスの処理過程において、外部に漏洩することがない。従って、電子チケットの権利証明を、紙によるチケットの場合と同様に、容易かつ安全に、第三者に対して行うことができる。

【００１９】

【発明が解決しようとする課題】

ところで、上述の特開平11-31204号公報においては、電子チケットの必要機能として、以下の３つの点が挙げられている。

【００２０】

即ち、第１点は、複製等によって正当な権利を持たないものにチケットを利用されることを防ぐ機能である「権利複製防止」であり、第２点は、身元などが特定されない匿名の者をも含む第三者に対して、電子チケットに基づく権利を証明する機能である「権利証明」であり、第３点は、電子チケットを利用する際（電子チケットに基づく権利を行使して、サービスの提供を受ける際）に、その利用者の匿名性を保証する機能である「匿名性」である。

【００２１】

これらの第１乃至第３点は、いずれも従来の紙によるチケットにおいて実現されている機能であり、電子チケットにおいても、紙によるチケットの利便性を損なわないように維持されるべきものである。

【００２２】

しかしながら、電子チケットにおいて、紙によるチケットと同様の利便性を確保するには、上述の３つの機能だけでは足りず、以下の、第４および第５の機能が必要であると考えられる。

【００２３】

即ち、第４点としては、電子チケットに基づく権利を他人に譲ることができる機能である「譲渡性」が必要であると考えられる。さらに、第５点としては、電子チケットの権利確認のために、つまり、「権利証明」を行うために、チケット管理センタや、管理データベース等へのアクセスをその都度必要とはしないという「完結性」が必要であると考えられる。

【００２４】

紙によるチケットは、それ自体を、他人に渡すことで、そのチケットに基づく権利を、他人に譲ることができる。従って、「譲渡性」は、紙によるチケットと同様の利便性を確保するために、必要不可欠の機能である。

【００２５】

また、例えば、鉄道駅やイベントの入場改札等においては、紙によるチケットの提示や受け渡し等によって、そのチケットに基づく権利を、即座に確認し、円滑な入場整理を行うことができる。従って、改札等において、例えば、クレジットカードのようなオンライン検査を必要としたり、あるいは、ある番号のチケットが何を意味するかをデータベースの一覧表から検索することを必要とするのでは、円滑な入場が妨げられることになり、「権利証明」を、電子チケットそれ自体で行うことのできる「完結性」は、電子チケットの現実的な利用を考えた場合には不可欠なものとなる。

【００２６】

しかしながら、上述の第２の方法では、「譲渡性」および「完結性」を満足す

ることは困難である。

【００２７】

即ち、第２の方法では、電子チケット（としての情報）は、個々の電子チケットごとに異なる特徴情報（例えば、上述の公開鍵暗号化方式の秘密鍵）を、個々の保持装置ごとに異なる暗号鍵で暗号化することにより発行される。さらに、第２の方法では、保持装置が保持している暗号化された特徴情報を、その保持装置が保持している暗号鍵でしか復号することができないようにして、「権利複製防止」を実現している。そして、第２の方法において、電子チケットについての「権利証明」は、保持装置が保持している暗号化された特徴情報を、その保持装置が保持している暗号鍵で復号し、その復号した特徴情報を用いて行われる。

【００２８】

以上から、第２の方法では、電子チケットが発行された保持装置でしか、その電子チケットの特徴情報を復号することができず、その結果、電子チケットが発行された保持装置以外の保持装置では、「権利証明」を行うことができない。このことは、ある保持装置に発行された電子チケットを、他の保持装置に譲ることができないこと、つまり、「譲渡性」に欠けることを意味する。

【００２９】

また、紙によるチケットは、そのチケットとしての紙に書かれている内容である「権利条項」と、印刷、材質、検印、透かしなどによって偽造および複製が困難な紙自体が表すチケットの「有効性」の２つの要素を有していると考えることができ、この「権利条項」と「有効性」は、印刷によって密接不可分に結びついている。つまり、「権利条項」自体は情報であるが、その「権利条項」が印刷された複製等の困難な紙という「有効性」があって、はじめて、チケットたり得る。

【００３０】

紙によるチケットは、「有効性」と「権利条項」の両方を、密接不可分に組み合わせたものとなっており、これによって、「権利複製防止」、「権利証明」、「匿名性」、「譲渡性」、および「完結性」の５つの機能が実現されている。

【００３１】

紙によるチケットが備える「有効性」と「権利条項」のうち、特に、「有効性

」については、紙によるチケットが有する特徴を維持したまま電子情報化するのが困難であり、このため、第２の方法では、紙によるチケットの「有効性」の特徴であるポータビリティ(portability)を犠牲にすることで、「権利複製防止」を実現している。つまり、第２の方法では、電子チケットの「有効性」を、特定の保持装置の存在と結び付け、「譲渡性」を犠牲にして、「権利複製防止」を実現している。

【００３２】

さらに、第２の方法では、「権利証明」において、上述のようなチャレンジアンドレスポンスの認証方法が用いられるが、その際、検査装置は、自身が発生した乱数に対する電子署名を生成するのに用いる秘密鍵を識別する識別番号を、保持装置に送信する。保持装置においては、上述のように、電子チケットごとに異なる特徴情報としての秘密鍵が、保持装置ごとに異なる暗号鍵で暗号化されており、保持装置は、検査装置から、識別番号を受信すると、その識別番号に対応する秘密鍵を検索する。そして、保持装置は、その秘密鍵を、保持装置に固有の暗号鍵で復号し、その秘密鍵で、検査装置からの乱数を処理することによって、電子署名を生成する。この電子署名は、保持装置から検査装置に送信され、検査装置は、その電子署名を、保持装置に送信した識別番号によって特定される秘密鍵に対応する公開鍵で処理する。そして、検査装置は、その処理結果に基づいて、電子署名の検証を行い、電子チケットに基づく権利の確認（検査）を行う。

【００３３】

このように、第２の方法では、チャレンジアンドレスポンスの認証方法を用いることによって、電子チケットに基づく権利を表す秘密鍵を外部に示すことなく、紙によるチケットと同様の安全な権利確認（「権利証明」）を行うことができる。

【００３４】

しかしながら、第２の方法では、電子チケットに基づく権利を、どのように確認（検証）するべきかという情報、つまり、上述の場合には、ある電子チケットに基づく権利を、チャレンジアンドレスポンスの認証方法によって確認するのに必要な情報は、電子チケットの情報とは別に用意されており、検査装置側で把握

しなければならない。

【００３５】

即ち、第２の方法においては、例えば、ある電子チケットに基づく権利を表す秘密鍵に対応する公開鍵と、その秘密鍵を識別する識別番号とが公開され、あるチケット管理センタに登録される。従って、検査装置は、ある電子チケットに基づく権利を確認する場合に、その権利を表す秘密鍵を識別する識別番号と、対応する公開鍵を、チケット管理センタにアクセスして取得する必要がある。

【００３６】

検査装置が確認する権利内容が、常に同一であれば、検査装置は、チケット管理センタにアクセスして、識別番号および公開鍵を、一度だけ取得すれば問題ないが、電子チケットが普及した場合を考えると、検査装置が確認する権利内容が、常に同一であることを前提とするのは非現実的である。

【００３７】

即ち、例えば、鉄道の切符を、電子チケットで実現した場合を考えると、改札として機能する検査装置は、各駅において日々発行され、さらには、普通電車や特急電車等によって権利内容が異なる電子チケットを検査しなければならない。従って、検査装置は、例えば、駅や、日、電車の種類ごとに異なる識別番号および公開鍵を、電子チケットの検査を行うたびに、チケット管理センタにアクセスして取得しなければならず、この場合、電子チケットの検査に時間を要することとなり、円滑な改札が妨げられることになる。これは、第２の方法において、電子チケットが、それ自体で、権利内容を確認することができるという「完結性」を欠いていることに起因する。

【００３８】

さらに、この「完結性」の欠如は、「譲渡性」の実現に影響を与える。即ち、電子チケットが「完結性」を有しない場合には、電子チケットの譲渡にあたって、その電子チケットが有効であるかどうかの検査を、上述のように、チケット管理センタにアクセスして確認しなければならないこととなる。従って、電子チケットに、その譲渡を可能とする機能を、単に追加したとしても、電子チケットが「完結性」を有しなければ、電子チケットが有効であるかどうかの検査が煩雑と

なり、このことは、電子チケットの譲渡を行うにあたって障害となる。

【００３９】

つまり、紙によるチケットであれば、一般に、その紙によるチケットを見ることによって、即座に、そのチケットの有効性を検査（確認）することができ、極端には、どのような相手からであっても、チケットが有効であるかどうかを、即座に確認して、その譲渡を受けることができる。

【００４０】

しかしながら、電子チケットが「完結性」を有しない場合には、譲渡にあたって、電子チケットが有効であるかどうかの検査を即座に行うことができず、電子チケットが、譲渡可能な機能を有していても、事実上、譲渡が行われないこととなる。即ち、電子チケットの譲渡が行われるのは、実際上、電子チケットの発行者から、ユーザに対してだけということになる。

【００４１】

本発明は、このような状況に鑑みてなされたものであり、「権利複製防止」、「権利証明」、および「匿名性」の他に、「譲渡性」および「完結性」をも有する、利便性の高い電子チケットを実現することができるようにするものである。

【００４２】

【課題を解決するための手段】

本発明の情報記録媒体は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報とが記録されていることを特徴とする。

【００４３】

本発明の第１の情報処理装置は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成手段と、秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成手段と、検証用パラメータを含み、有効性データによって

、その有効性が証明される被証明情報を生成する被証明情報生成手段と、有効性データと被証明情報とからなる情報セットを外部に出力する出力手段とを備えることを特徴とする。

【００４４】

本発明の第１の情報処理方法は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成ステップと、秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成ステップと、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成ステップと、有効性データと被証明情報とからなる情報セットを外部に出力する出力ステップとを備えることを特徴とする。

【００４５】

本発明の第１のプログラム記録媒体は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成ステップと、秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成ステップと、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成ステップと、有効性データと被証明情報とからなる情報セットを外部に出力する出力ステップとを備えるプログラムが記録されていることを特徴とする。

【００４６】

本発明の第２の情報処理装置は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を、その被証明情報を検査する検査装置に送信する被証明情報送信手段と、秘密情報の存在を証明する証明データを生成し、検査装置に送信する証明データ生成手段とを備えることを特徴とする。

【００４７】

本発明の第２の情報処理方法は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を、その被証明情報を検査する検査装置に送信する被証明情報送信ステップと、秘密情報の存在を証明する証明データを生成し、検査装置に送信する証明データ生成ステップとを備えることを特徴とする。

【００４８】

本発明の第２のプログラム媒体は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を、その被証明情報を検査する検査装置に送信する被証明情報送信ステップと、秘密情報の存在を証明する証明データを生成し、検査装置に送信する証明データ生成ステップとを備えるプログラムが記録されていることを特徴とする。

【００４９】

本発明の第３の情報処理装置は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を受信する被証明情報受信手段と、秘密情報の存在を証明する証明データを受信する証明データ受信手段と、証明データと、被証明情報に含まれる検証用パラメータとを用いて、他の装置における秘密情報の存否を判定する存否判定手段とを備えることを特徴とする。

【００５０】

本発明の第３の情報処理方法は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情

報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を受信する被証明情報受信ステップと、秘密情報の存在を証明する証明データを受信する証明データ受信ステップと、証明データと、被証明情報に含まれる検証用パラメータとを用いて、他の装置における秘密情報の存否を判定する存否判定ステップとを備えることを特徴とする。

【００５１】

本発明の第３のプログラム記録媒体は、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を受信する被証明情報受信ステップと、秘密情報の存在を証明する証明データを受信する証明データ受信ステップと、証明データと、被証明情報に含まれる検証用パラメータとを用いて、他の装置における秘密情報の存否を判定する存否判定ステップとを備えるプログラムが記録されていることを特徴とする。

【００５２】

本発明の情報処理システムは、第１の情報処理装置が、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データを生成する有効性データ生成手段と、秘密情報が存在することを検証するのに用いられる検証用パラメータを生成する検証用パラメータ生成手段と、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報を生成する被証明情報生成手段と、有効性データと被証明情報とからなる情報セットを外部に出力する出力手段とを備え、第２の情報処理装置が、情報セットを記憶する記憶手段と、被証明情報を、その被証明情報を検査する第３の情報処理装置に送信する被証明情報送信手段と、秘密情報の存在を証明する証明データを生成し、第３の情報処理装置に送信する証明データ生成手段とを備え、第３の情報処理装置が、第２の情報処理装置からの被証明情報を受信する被証明情報受信手段と、第２の情報

処理装置からの秘密情報の存在を証明する証明データを受信する証明データ受信手段と、証明データと、被証明情報に含まれる検証用パラメータとを用いて、第２の情報処理装置における有効性データの存否を判定する存否判定手段とを備えることを特徴とする。

【００５３】

本発明の情報記録媒体においては、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報とが記録されている。

【００５４】

本発明の第１の情報処理装置および情報処理方法、並びにプログラム記録媒体においては、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データが生成されるとともに、秘密情報が存在することを検証するのに用いられる検証用パラメータが生成される。そして、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が生成され、有効性データと被証明情報とからなる情報セットが発行される。

【００５５】

本発明の第２の情報処理装置および情報処理方法、並びにプログラム記録媒体においては、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が、その被証明情報を検査する検査装置に送信される。さらに、秘密情報の存在を証明する証明データが生成され、検査装置に送信される。

【００５６】

本発明の第３の情報処理装置および情報処理方法、並びにプログラム記録媒体においては、それ自体を外部に示すことなく、それが存在することを証明するこ

とができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が受信されるとともに、秘密情報の存在を証明する証明データが受信される。そして、証明データと、被証明情報に含まれる検証用パラメータとを用いて、他の装置における秘密情報の存否が判定される。

【００５７】

本発明の情報処理システムにおいては、第１の情報処理装置において、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データが生成されるとともに、秘密情報が存在することを検証するのに用いられる検証用パラメータが生成される。さらに、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が生成され、有効性データと被証明情報とからなる情報セットが発行される。第２の情報処理装置では、被証明情報が、その被証明情報を検査する第３の情報処理装置に送信されるとともに、秘密情報の存在を証明する証明データが生成され、第３の情報処理装置に送信される。第３の情報処理装置では、第２の情報処理装置からの被証明情報が受信されるとともに、第２の情報処理装置からの有効性データの存在を証明する証明データが受信され、証明データと、被証明情報に含まれる検証用パラメータとを用いて、第２の情報処理装置における秘密情報の存否が判定される。

【００５８】

【発明の実施の形態】

図１は、本発明を適用した電子チケットシステム（システムとは、複数の装置が論理的に集合した物をいい、各構成の装置が同一筐体中に存在するか否かは問わない）の一実施の形態の構成例を示している。

【００５９】

この電子チケットシステムは、チケット管理センタ１、チケット発行者が有するチケット発行装置3_1，3_2，・・・，3_T、ユーザが有するチケット保持装置4_1，4_2，・・・，4_U、およびサービス提供者が有するチケット検査装置5_1，

5_2，・・・，5_Sが、相互に、ネットワーク２を介して接続されることにより構成されている。

【００６０】

チケット管理センタ１は、電子署名の認証センタとして機能する。

【００６１】

ネットワーク２は、例えば、公衆回線、インターネット、ＣＡＴＶ(Cable Television)網、地上波、衛星回線等で構成される。

【００６２】

チケット発行者が有するチケット発行装置3_tは、電子チケット（厳密には、電子チケットの実体となる情報（電子チケット情報））を発行し、ユーザが有するチケット保持装置4_uに提供する。

【００６３】

なお、チケット発行装置3_tにおいて、電子チケットの提供は、チケット保持装置4_uとネットワーク２を介して通信することにより行うことも可能であるし、チケット保持装置4_uと直接に、無線または有線で通信することにより行うことも可能である。また、チケット保持装置4_uのユーザは、必要に応じて、チケット発行装置3_tに対して電子チケットの提供（譲渡）に対する対価として、その電子チケットの代金を支払う。この電子チケットの代金の支払いのための課金処理は、ネットワーク２を介して行うことも可能であるし、チケット発行装置3_tとチケット保持装置4_uとの間で、直接に通信することによって行うことも可能である。さらに、電子チケットの代金の支払いは、その代金を、チケット発行装置3_tに直接投入して行うことも可能である。

【００６４】

ユーザが有するチケット保持装置4_uは、チケット発行装置3_tが発行する電子チケット（の実体である電子チケット情報）を保持する。ユーザは、このチケット保持装置4_uが保持する電子チケットに基づく権利を行使することができ、これにより、チケット検査装置5_sを有するサービス提供者（チケット発行装置3_tを有するチケット発行者と同一である場合もある）から、その権利に対応するサービスの提供を受けることができる。

【００６５】

なお、ユーザは、チケット保持装置４$_u$どうしの間で通信を行うことにより、電子チケット（に基づく権利）を授受することができる。この電子チケットの授受は、電子チケットが使用される前に行うことができる他、電子チケットが、有効期限や使用回数の制限のあるものである場合には、使用された後であっても、有効期限が切れる前や、使用回数の制限を越える前であれば行うことができる。また、チケット保持装置４$_u$は、有効期限が切れた電子チケットや、使用回数制限を越えた電子チケット等の不要な電子チケットを破棄することができる。さらに、チケット保持装置４$_u$では、複数の電子チケットを保持することができる。

【００６６】

サービス提供者が有するチケット検査装置５$_s$は、チケット保持装置４$_u$が保持する電子チケットの検査（検証）を行う。なお、電子チケットの検査も、チケット発行装置３$_t$からチケット保持装置４$_u$に対する電子チケットの提供（譲渡）と同様に、ネットワーク２を介して行うことも可能であるし、チケット保持装置４$_u$とチケット検査装置５$_s$との間で、直接通信することによって行うことも可能である。

【００６７】

なお、チケット管理センタ１、チケット発行装置３$_t$、チケット保持装置４$_u$、およびチケット検査装置５$_s$は、いずれも、例えば、コンピュータで構成することが可能である。また、例えば、チケット保持装置４$_u$は、ＩＣ(Integrated Curcuit)カードで構成し、チケット発行装置３$_t$およびチケット検査装置５$_s$は、ＩＣカードのリーダ／ライタで構成することも可能である。さらに、チケット保持装置４$_u$は、例えば、携帯電話機や、ＰＤＡ(Personal Digital Assistant)等の携帯端末で構成することも可能である。

【００６８】

以上のように構成される電子チケットシステムにおいては、上述の「権利複製防止」、「権利証明」、「匿名性」、「譲渡性」、および「完結性」の５つの機能すべてを有する電子チケットを流通させることができるようになっている。

【００６９】

即ち、図１の電子チケットシステムで対象とする電子チケットは、複製できないが、移動が可能な「有効性」と、それに結びついた「権利条項」とから構成され、さらに、個々の電子チケットは、それぞれ異なる「有効性」を有する。

【００７０】

電子チケットの「有効性」を表す情報は、例えば、電子署名を生成するのに用いられる情報（例えば、公開鍵暗号化方式の秘密鍵、ゼロ知識証明の可能な情報など）などの、認証によってその存在が確認できるが、それ自体は外部に漏れない（示されない）性質を有する情報（秘密情報）と、後述する付加情報とから構成される。

【００７１】

「有効性」を表す情報は、チケット保持装置4_uにおいて、後述する手法により、複製や改竄をすることができないように保持される。また、「有効性」を表す情報は、そのチケット保持装置4_uを有するユーザでさえも知ることができない。

【００７２】

「権利条項」を表す情報は、従来の紙によるチケットに書かれている情報に相当する。従って、電子チケットが、例えば、イベントチケットの場合には、「権利条項」を表す情報は、開催日時や、場所、イベント名などから構成される。但し、電子チケットにおいては、「権利条項」を表す情報には、「有効性」を表す情報の存在を検証するのに用いられるパラメータ（検証用パラメータ）も含まれる。即ち、例えば、「有効性」を表す情報が、電子署名を生成するのに用いられる公開鍵暗号化方式の秘密鍵である場合には、「権利条項」を表す情報には、その秘密鍵に対応する公開鍵が含まれる。

【００７３】

さらに、「権利条項」を表す情報には、その電子チケットのチケット発行者の証明書（後述する発行者証明書）と、チケット発行者による電子署名とが含まれる。ここで、「権利条項」に含まれるチケット発行者の証明書は、電子チケットのチケット発行者と、「有効性」の存在を検証するのに用いられる公開鍵との対応を証明し、これにより、「権利条項」の改竄を防止するとともに、「権利条項

」と、対応する「有効性」との関係を変更することを防止する。

【００７４】

電子チケットを構成する「権利条項」は、上述のように、紙によるチケットに書かれている情報に相当し、それ自体は、電子チケットに基づく権利の内容を表すものであるが、電子チケットとしての正当性（有効性）を証明するには、「有効性」の存在が必要となる。そして、「有効性」を表す情報は、上述のように、その存在を証明するにあたって、外部に示されない。

【００７５】

従って、電子チケットに基づく権利の内容は、「権利条項」を示す（出力する）ことで、任意の第三者に認識させることができ、さらに、その権利が有効なものかどうかは、外部には示されない「有効性」の存在によって証明されるから、「権利条項」を表す情報自体は、仮に、悪意の第三者に複製されたとしても、「有効性」が存在しない限り、電子チケットが複製されたことにはならない。その結果、「権利条項」を表す情報は、第三者による複製を心配せずに扱うことができる。

【００７６】

以上のような「有効性」と「権利条項」の組からなる電子チケットを実現するために、チケット管理センタ１は、チケット発行者の証明書（発行者証明書）を発行する認証センタとして機能する。

【００７７】

即ち、チケット管理センタ１は、電子署名を生成する秘密鍵としての署名生成用秘密鍵S_{CA}と、その秘密鍵に対応する公開鍵としての署名検証用公開鍵P_{CA}を有している。署名生成用秘密鍵S_{CA}は、外部には一切秘密にされ、署名検証用公開鍵P_{CA}は、ネットワーク２を介して、誰でも取得することができるように公開される。

【００７８】

そして、チケット管理センタ１は、署名生成用秘密鍵S_{CA}を用いて、発行者証明書を生成し、チケット発行者に対して発行する。このように、発行者証明書は、チケット管理センタ１だけが知り得る署名生成用秘密鍵S_{CA}を用いて生成され

るため、チケット管理センタ１だけが発行することができる。この発行者証明書と、後述するチケット発行者の署名によって、チケット発行者以外の者が、そのチケット発行者が発行した電子チケットを改竄することが防止される。

【００７９】

電子チケットについては、「発行」、「行使」、「譲渡」、および「破棄」の４つの操作が可能となっている。

【００８０】

電子チケットの「発行」は、チケット発行装置3_tで行われるが、その発行時に、電子チケットを所有する者（チケット保持装置4_u）を特定する情報を、電子チケットに含める必要はない。その結果、チケット発行装置3_tが発行し、あるチケット保持装置4_uに譲渡した電子チケットは、「譲渡」によって、そのチケット保持装置4_uから他のチケット保持装置$4_{u'}$に移動することができる。つまり、紙によるチケットにおける場合と同様に、電子チケットを譲渡することができる。

【００８１】

電子チケット（に基づく権利）の「行使」は、チケット保持装置4_uから、電子チケットの「権利条項」の情報を、サービス提供者のチケット検査装置5_sに出力し、さらに、チケット検査装置5_sに対して、その「権利条項」の情報の有効性を証明する「有効性」の情報が、チケット保持装置4_uに存在することを証明することによって行われる。

【００８２】

即ち、チケット検査装置5_sは、チケット保持装置4_uからの「権利条項」の情報の正当性（改竄されていないかどうか）を確認し、それに対応するサービスを提供することができるのであれば、その「権利条項」の情報、つまりは電子チケット自体の有効性を証明する「有効性」の情報がチケット保持装置4_uに存在するかどうかの確認を行う。

【００８３】

「有効性」の情報が存在することの確認は、チケット保持装置4_uから見れば、「権利証明」を行うことになる。この「権利証明」は、例えば、チャレンジア

ンドレスポンスの認証方法によって行われる。即ち、チケット検査装置５$_s$は、チケット保持装置４$_u$に乱数を送信し、チケット保持装置４$_u$は、その乱数から、「有効性」の情報を用いて、電子署名を生成し、チケット検査装置５$_s$に返す。チケット検査装置５$_s$は、チケット保持装置４$_u$からの電子署名と、元の乱数との一致性を判断することにより、電子署名の認証を行う。そして、チケット検査装置５$_s$は、その認証が成功すれば、チケット保持装置４$_u$に「権利条項」の情報に対応する「有効性」の情報が存在するとして、即ち、そのチケット保持装置４$_u$が保持している電子チケットが有効であるとして、その電子チケットに基づく権利の行使を認める。これにより、サービス提供者は、チケット保持装置４$_u$のユーザに対して、所定のサービスを提供する。

【００８４】

このように、「権利証明」は、チャレンジアンドレスポンスの認証方法によって行われるため、「有効性」の情報は、チケット保持装置４$_u$の外部に漏れることはない。従って、「権利証明」を、不特定の第三者に対して、電子チケットに基づく権利を安全に保ちながら（複製を防止し、さらには、盗まれる心配をせずに）行うことができる。

【００８５】

ここで、紙によるチケットには、大きく分けて、権利証明書として何回でも反復使用ができるものと、乗車券、回数券等のように使用回数が制限されるもの、あるいは定期券などのように使用期間が限定されるものとの２種類が存在する。

【００８６】

電子チケットにおいても、紙によるチケットと同様に、反復使用ができるものと、使用回数または使用期間が限定されているものの２種類の実現が可能である。

【００８７】

即ち、例えば、使用回数が限定された電子チケットは、その電子チケットの使用回数と、その使用回数の制限値とを、電子チケットに含めることにより実現することが可能である。そして、サービス提供者において、チケット検査装置４$_s$によって、電子チケットの使用回数とその制限値とを比較し、使用回数が制限値

を越えている場合には、サービスの提供を拒否すれば良い。

【００８８】

なお、この場合、使用回数が限定された電子チケットについて、使用回数が制限値を越えているときには、その電子チケットを無効とする必要があるが、そのためには、使用回数が制限値を越えているかどうかを判断する必要がある。従って、使用回数および制限値は、その改竄をすることができないように、電子チケットに書き込む必要がある。

【００８９】

また、使用期限が制限された電子チケットも、その使用期限を電子チケットに含めることで実現することが可能である。

【００９０】

ところで、例えば、新幹線の特急券を、電子チケットで実現する場合を考えてみると、一度使用を開始した特急券を使用して、別の新幹線に乗車することを制限する他、その電子チケットで乗車した新幹線において、新幹線に乗車することの権利を証明するのに、特急券を車掌等に提示できることが必要である。

【００９１】

従って、電子チケットについては、その使用回数の制限値は勿論、その使用回数、あるいは、電子チケットを使用したかどうか（電子チケットに基づく権利を行使したかどうか）を、サービス検査装置5_Sが認識することができることが重要である。

【００９２】

そこで、ここでは、電子チケットに基づく権利の行使、即ち、チケット保持装置4_u側からすれば「権利証明」を、２つの方法によって行うことが可能となっている。

【００９３】

即ち、第１の「権利証明」の方法は、上述したように、チケット保持装置4_uに「有効性」の情報が存在することだけを証明することによる、いわば「通常の権利証明」であり、第２の「権利証明」の方法は、チケット保持装置4_uに「有効性」の情報が存在することと、使用回数とを証明することによる、いわば「回

数付き権利証明」である。

【００９４】

「回数付き権利証明」も、基本的には、「通常の権利証明」と同様に、チャレンジアンドレスポンスの認証方法によって行うことができる。但し、「回数付き権利証明」を行う場合には、チケット保持装置４$_u$は、チケット検査装置５$_t$から送信されてくる乱数だけではなく、その乱数と、電子チケットに含まれる使用回数との組に対して、電子署名を生成し、その電子署名と使用回数との組を、チケット検査装置５$_s$に返す。チケット検査装置５$_s$は、チケット保持装置４$_u$からの電子署名と使用回数を用いて、「有効性」の情報の存在と、使用回数とを確認する。

【００９５】

なお、「通常権利証明」と「回数付き権利証明」のうちのいずれを行うかは、例えば、ユーザが、チケット保持装置４$_u$を操作することによって決定することができる。

【００９６】

次に、電子チケットの「譲渡」については、あるチケット保持装置４$_u$（あるいは、チケット発行装置３$_t$）が有する電子チケットを構成する「有効性」と「権利条項」の両方の情報を、他のチケット保持装置４$_{u'}$に移動することによって行われる。なお、「有効性」の情報は、譲渡側の装置と譲受側の装置との間で唯一性を保ちながら移動される。即ち、「有効性」の情報は、その移動途中で複製されないように移動される。

【００９７】

電子チケットの「破棄」については、「有効性」と「権利条項」の両方の情報を削除することで実現される。なお、この「破棄」は、電子チケットを譲渡した場合に、その譲渡側の装置で行われる他、電子チケットを保持しているチケット保持装置４$_u$やチケット発行装置３$_t$において、例えば、有効期限や使用回数の制限値から、電子チケットが無効になったことが判明した場合も行われる。

【００９８】

ところで、電子チケットにおける電子化された「有効性」の情報は、紙による

チケットが有する「有効性」と比較して、複製が容易である。

【００９９】

電子チケットの「行使」においては、チャレンジアンドレスポンスの認証方法を用いることで、「有効性」の情報の存在を、その情報自体を外部に示すことなく証明することができるから、「権利証明」を行う際に、「有効性」の情報が複製されることは防止することができる。

【０１００】

しかしながら、「有効性」の情報の複製は、「権利証明」時だけでなく、電子チケットがチケット保持装置４$_u$に保持されている状態、および電子チケットの譲渡に際し、「有効性」の情報が移動中の状態においても防止する必要がある。

【０１０１】

このような「有効性」の情報の複製の防止は、電子チケットの利便性を考慮すれば、パーソナルコンピュータ等の汎用の情報処理装置であっても、最小限の機能追加で行うことができるのが望ましい。

【０１０２】

最近では、音楽情報のネットワーク配信の普及に伴い、音楽情報を複製されないように移動し、保持するための技術が提案されている。従って、電子チケットにおける「有効性」の情報についても、この技術を取り入れて、その複製を防止することが可能である。

【０１０３】

即ち、音楽情報は、例えば、MP3(MPEG(Moving Picture Expert Group)1 Audio Layer 3)やATRAC(Adaptive TRansform Acoustic Coding)等といった汎用的な音楽情報圧縮形式に圧縮されるが、このように圧縮された音楽情報を複製することができた場合には、それを伸長して、容易に利用することができる。このため、音楽情報等（以下、コンテンツという）は、暗号化などの手法を用いて処理され、これにより、移動時や保持時において、仮に、その複製が行われたとしても、それを利用することができないようにすることで、結果として、不正な複製が防止されるようになっている。

【０１０４】

このように、コンテンツを不正な複製から保護する方法としては、例えば、特開平11-328850号公報に記載されているように、暗号化されたコンテンツ、その暗号を復号するコンテンツ鍵、およびコンテンツを保持する装置に固有の固有鍵を管理するハードウェアである管理回路を用いるものがある。この方法では、コンテンツは、暗号化して保持され、そのまま読み出しても利用できないものとされる。さらに、コンテンツ鍵は、固有鍵によって暗号化され、管理回路に保持されており、コンテンツを復号するときのみ、固有鍵を用いて復号される。また、コンテンツの移動は、盗聴を避けるために暗号化された状態で行われ、コンテンツの移動が行われた場合には、移動元の装置におけるコンテンツは、管理回路によって確実に削除される。管理回路は、いわゆる耐タンパー性を有し、これにより、管理回路が保持する鍵の取り出しや改竄が防止されるようになっている。

【０１０５】

以上のように、コンテンツを保護しながら取り扱うことが可能な実用システムとしては、例えば、本件出願人が開発したMagic Gateシステム等がある。

【０１０６】

電子チケットの「有効性」の情報について、唯一性を維持するには、上述のような、コンテンツを、その複製を防止しながら保持および移動する方法を利用することができる。「有効性」の情報は、音楽情報等のコンテンツに比べて、サイズが小さく、また、固定サイズとすることが可能であり、処理が容易である。さらに、「有効性」の情報を復号するのは、「権利証明」を行うときに限られるから、その盗聴や改竄を防止するのも、コンテンツに比較して容易である。また、電子チケットを保持する装置において、管理回路と、「権利証明」のための電子署名を生成する回路とを、ハードウェア的に一体に構成すること等によって、復号された「有効性」の情報の漏洩を比較的容易に防止することができる。従って、「有効性」の情報は、復号後のデータを、他の装置に移動して処理することがあるコンテンツに比較して有利である。

【０１０７】

以上のように、図１の電子チケットシステムにおいて流通する電子チケットは、一対一の対応関係にある「有効性」と「権利条項」の情報から構成され、その

うちの「有効性」の情報の唯一性を、チケット保持装置４$_u$のハードウェア機能等を利用して維持することによって、第１点の「権利複製防止」を実現することができる。さらに、「有効性」の情報の存在を示す仕組みによって、第２点の「権利証明」を行うことが可能であり、その際、チケット保持装置４$_u$を特定する情報を必要としないことによって、第３点の「匿名性」を実現することができる。そして、「有効性」の情報を、その唯一性を保ちながら移動することによって、第４点の「譲渡性」を実現することができる。さらに、「権利条項」の情報に、十分な情報を含ませ、かつ「権利証明」の機能を利用することによって、第５点の「完結性」を実現することが可能となる。

【０１０８】

次に、図２および図３を参照して、図１のチケット管理センタ１の役割について説明する。

【０１０９】

チケット管理センタ１は、上述したように、電子署名の認証センタとして機能する。

【０１１０】

即ち、チケット管理センタ１は、例えば、公開鍵暗号化方式を利用して、電子署名付きの証明書を発行する。

【０１１１】

ここで、公開鍵暗号化方式は非対称暗号化方式とも呼ばれ、データを暗号化する際に用いられる鍵と、その暗号を復号する際に用いられる鍵が異なり、さらに、一方の鍵から他方の鍵を算出することが非常に困難であるという性質を持った暗号アルゴリズムである。一般に、暗号化の鍵は、第三者に公開されることから公開鍵と呼ばれ、復号の鍵は、第三者に秘密にされることから秘密鍵と呼ばれる。

【０１１２】

公開鍵暗号化方式によれば、秘密鍵が知られない限り、その秘密鍵に対応する公開鍵や、公開鍵で暗号化されたデータ（暗号）が知られたとしても、元のデータ（公開鍵で暗号化される前のデータ）を得ることはできない。このような公開

鍵暗号化方式としては、例えば、RSA(R. L. Rivest, A. Shamir, L. Adleman)暗号、楕円曲線暗号などが知られている。

【０１１３】

いま、あるユーザ＃ｕに割り当てられた公開鍵と秘密鍵を、それぞれをP_uとS_uとして、公開鍵P_uによるデータMの暗号化を、C=E(P_u,M)と表すとともに、秘密鍵S_uによる暗号Cの復号を、M=D(S_u,C)と表すこととする。

【０１１４】

電子署名は、データを作成したユーザ＃ｕが、そのデータを、自分の秘密鍵S_uで復号処理することによって生成される。即ち、データMを作成したユーザ＃ｕは、自分の秘密鍵S_uを用いて、式SG(M)=D(S_u,h(M))を計算し、この計算結果SG(M)が電子署名となる。

【０１１５】

ここで、h()は一方向性関数（ハッシュ関数）であり、出力値から入力値を知ることが非常に困難であるという性質を有する。一方向性関数としては、例えば、MD5(Message Digest 5)やSHA-1(Secure Hashing Algorithm 1)などが知られている。

【０１１６】

ユーザ＃ｕは、データMを、そのデータMと電子署名SG(M)とのデータセット(M,SG(M))にして送信する。このデータセット(M,SG(M))を受信した受信側では、ユーザ＃ｕの公開されている公開鍵P_uを用いて、データセット(M,SG(M))における電子署名SG(M)を暗号化処理し、その暗号化結果E(P_u,SG(M))と、データセット(M,SG(M))におけるデータMを引数として一方向性関数h()を計算した計算結果h(M)との一致性が認められるかどうか、即ち、式h(M)=E(Pk,SG(M))が満たされるかどうかを確認する。この一致性が満たされることによって、データMが改竄されていないこと、および電子署名SG(M)が秘密鍵S_uのユーザ＃ｕによって付加されたことを確認することできる。電子署名としては、RSA署名やElGamal署名、楕円ElGamal署名などが知られている。

【０１１７】

ここで、以上のようにして、データMが改竄されていないことや、電子署名SG(

M)が秘密鍵S_uのユーザ＃ｕによって付加されたことを確認することを、以下、適宜、署名確認という。また、署名確認を行うには、一方向性関数h()を知る必要があるが、以下においては、署名確認に用いられる一方向性関数h()を特定する情報は、公開鍵P_uに含まれているものとする。

【０１１８】

公開鍵暗号化方式によれば、以上のような署名確認を行う他、ユーザ＃ｕが秘密鍵S_uを所有していること（秘密鍵S_uの存在）を、チャレンジアンドレスポンスの手法によって、秘密鍵S_u自体を知ることなく確認（検証）することができる。

【０１１９】

即ち、ユーザ＃ｕが秘密鍵S_uを所有していることを検証する検証側は、例えば、乱数r（チャレンジ）を発生し、その乱数rを、ユーザ＃ｕの公開鍵P_uで暗号化して、暗号$r'=E(P_u,r)$を求める。検証側は、この暗号r'を、ユーザ＃ｕに送り、ユーザ＃ｕは、暗号r'を、秘密鍵S_uで復号し、その復号結果$D(S_u,r')$（レスポンス）を、検証側に返す。検証側は、ユーザ＃ｕからの復号結果$D(S_u,r')$が、自身が発生した乱数rに等しいかどうかを判定し、等しければ、即ち、式$r=D(S_u,r')$が成立すれば、ユーザ＃ｕが、秘密鍵S_uを所有していることを確認（検証）することができる。

【０１２０】

また、検証側では、乱数rそのものを、ユーザ＃ｕに送り、ユーザ＃ｕには、その乱数rから一方向性関数h()を計算した値h(r)を、ユーザ＃ｕの秘密鍵S_uで復号処理した復号処理結果$r''=D(S_u,h(r))$を求めさせることができる。この場合、検証側は、その復号処理結果r''を、ユーザ＃ｕの公開鍵P_uで暗号化して、その暗号化処理結果$E(P_u,r'')$が、乱数rから一方向性関数h()を計算した値h(r)に等しいかどうかを判定することで、即ち、式$h(r)=E(P_u,r'')$が成り立つかどうかを判定することで、ユーザ＃ｕが、秘密鍵S_uを所有していることを確認することができる。

【０１２１】

なお、電子署名によっても、ユーザ＃ｕが、電子署名を生成するための秘密鍵S_uを所有しているかどうかを、上述の場合と同様にして、秘密鍵S_u自体を知るこ

となく確認することができる。即ち、検証側は、乱数rを生成して、ユーザ＃ｕに送信し、ユーザ＃ｕは、乱数rから、秘密鍵S_uを用いて電子署名SG(r)=D(Sk,h(r))を計算して、検証側に返す。検証側は、ユーザ＃ｕの公開鍵P_uを用いて、電子署名SG(r)を暗号化処理し、その暗号化処理結果$E(P_u,SG(r))$を求める。さらに、検証側は、式$h(r)=E(P_u,SG(r))$が成立するかどうかを判定し、成立すれば、ユーザ＃ｕが秘密鍵S_uを所有していることを確認することができる。

【０１２２】

以上のように、ユーザ＃ｕが、特定の秘密鍵S_uを所有していることを、その秘密鍵S_uに対応する公開鍵P_uを用いて確認することができるが、以下、適宜、この確認を、認証という。

【０１２３】

署名確認や認証を行うには、その対象とする相手が所有する秘密鍵に対応する公開鍵を認識する必要がある。しかしながら、署名確認や認証を行う対象とする相手が多数の場合には、その多数の公開鍵を認識していなければならず、面倒である。そこで、ある１つの公開鍵を認識していれば、その公開鍵を用いて、他の公開鍵を連鎖的に認識することができる方法が、ITU-T(International Telecommunications Union - Telecommunications Standardization Sector)のX.509勧告において規定されている。

【０１２４】

この認識していればよい公開鍵と、その公開鍵に対応する秘密鍵との所有者が認証センタ(CA(Certificate Authority))であり、チケット管理センタ１は、このような認証センタとして機能する。

【０１２５】

従って、チケット管理センタ１は、自身の公開鍵と、対応する秘密鍵とを有するが、この公開鍵と秘密鍵を、それぞれP_{CA}とS_{CA}と表す。公開鍵P_{CA}は、広く第三者に公開されるが、秘密鍵S_{CA}は、チケット管理センタ１以外には秘密にされる。

【０１２６】

そして、ある所有者＃ｎの公開鍵と秘密鍵を、それぞれP_nとS_nと表すと、チケ

ット管理センタ１は、所有者＃ｎから、その所有者＃ｎを識別する識別情報$Info_n$と、公開鍵P_nを受信し、その組$(Info_n,P_n)$に対し、自身の秘密鍵S_{CA}を用いて、電子署名$SG_n= D(S_{CA},h(Info_n,P_n))$を生成する。さらに、チケット管理センタ１は、所有者＃ｎからの識別情報$Info_n$および公開鍵P_nに対して、電子署名SG_nを付加することにより、証明書$(Info_n,P_n,SG_n)$を発行する。この証明書$(Info_n,P_n,SG_n)$は、チケット管理センタ１が、識別情報$Info_n$で特定される所有者＃ｎと、その所有者＃ｎの公開鍵P_nとの関係を保証するものとなる。

【０１２７】

即ち、所有者＃ｎは、証明書$(Info_n,P_n,SG_n)$を、公開鍵とその所有者との関係を検証する検証側に対して送信し、検証側は、公開されているチケット管理センタ１の公開鍵P_{CA}を用い、証明書$(Info_n,P_n,SG_n)$の電子署名SG_nについて、署名確認を行う。これにより、証明書$(Info_n,P_n,SG_n)$における識別情報$Info_n$と公開鍵P_nが改竄されていないこと、即ち、証明書$(Info_n,P_n,SG_n)$の正当性を確認することができる。そして、証明書$(Info_n,P_n,SG_n)$の正当性が確認されれば、証明書$(Info_n,P_n,SG_n)$における識別情報$Info_n$によって識別される所有者＃ｎが、公開鍵P_nを所有していることを確認することができる。従って、例えば、識別情報$Info_n$が人名である場合には、証明書$(Info_n,P_n,SG_n)$によれば、公開鍵P_nで認証を行うことができる相手の人名$Info_n$を確認することができる。

【０１２８】

なお、証明書には、一般に、暗号化のアルゴリズムや、使用されている一方向性関数h()の種類の情報も含まれる。また、上述の場合には、チケット管理センタ１において、識別情報$Info_n$および公開鍵P_nの組$(Info_n,P_n)$に対して、電子署名SG_nを生成するようにしたが、公開鍵P_nを所有する所有者＃ｎを確認する必要がない場合には、公開鍵P_nに対して、電子署名SG_nが生成され、公開鍵P_nに、電子署名SG_nを付加した証明書(P_n,SG_n)が発行される。この証明書(P_n,SG_n)は、公開鍵P_nで認証を行うことができる相手が、認証センタであるチケット管理センタ１に登録されている正当なものであることを確認するのに用いることができる。

【０１２９】

チケット発行装置３_tは、図２に示すように、そのチケット発行装置３_tを有す

るチケット発行者を識別する発行者識別情報TID_t、およびチケット発行者の電子署名を生成するのに用いられる秘密鍵としての発行者署名生成用秘密鍵$TSSK_t$と、その電子署名の署名確認（検証）に用いられる公開鍵としての発行者検証用公開鍵$TSPK_t$とのセットを有しており、そのうちの発行者識別情報TID_tと発行者署名検証用公開鍵$TSPK_t$を、あらかじめ、チケット管理センタ１に送信して、登録を要求する。

【０１３０】

チケット管理センタ１は、上述のように、電子署名を生成するのに用いられる秘密鍵としての署名生成用秘密鍵S_{CA}と、その電子署名の署名確認に用いられる公開鍵としての署名検証用公開鍵P_{CA}を有しており、チケット発行装置３_tからの発行者識別情報TID_tと発行者署名検証用公開鍵$TSPK_t$を登録した上で、その発行者識別情報TID_tと発行者署名検証用公開鍵$TSPK_t$に対して、署名生成用秘密鍵S_{CA}を用いて電子署名TSG_tを生成する。さらに、チケット管理センタ１は、チケット発行装置３_tからの発行者識別情報TID_tと発行者署名検証用公開鍵$TSPK_t$に対して、電子署名TSG_tを付加し、これにより、発行者識別情報TID_tによって識別されるチケット発行者と、発行者署名検証用公開鍵$TSPK_t$との対応関係を証明（保証）する証明書としての発行者証明書$TP_t(=(TID_t,TSPK_t,TSG_t))$を発行し、チケット発行装置$３_t$に送信する。

【０１３１】

チケット発行装置３_tは、このようにして、チケット管理センタ１から発行される発行者証明書TP_tを、あらかじめ内蔵している。

【０１３２】

チケット保持装置４_uには、図３に示すように、そのチケット保持装置４_uが、図１の電子チケットシステムの正当な参加機器であることを証明するのに用いられる秘密鍵としての装置証明用秘密鍵ASK_uと、チケット保持装置４_uが、図１の電子チケットシステムの正当な参加機器であることを検証するのに用いられる公開鍵としての装置検証用公開鍵APK_uとのセットが、あらかじめ内蔵されている。

【０１３３】

さらに、装置検証用公開鍵APK_uは、あらかじめチケット管理センタ１に送信さ

れて登録される。また、チケット管理センタ１は、装置検証用公開鍵APK_uに対して、署名生成用秘密鍵S_{CA}を用いて電子署名ASG_uを生成し、装置検証用公開鍵APK_uに対して、電子署名TSG_tを付加することにより、装置検証用公開鍵APK_uに対応する装置証明用秘密鍵ASK_uを有しているチケット保持装置４$_u$が、正当なものであることを証明する証明書としての装置証明書$AP_u(=(APK_u, ASG_u))$を発行する。

【０１３４】

チケット保持装置４$_u$は、このようにして、チケット管理センタ１から発行される装置証明書AP_uを、あらかじめ内蔵している。

【０１３５】

次に、図４は、チケット発行装置３$_t$が発行する電子チケットの実体としての電子チケット情報のフォーマットを示している。

【０１３６】

電子チケット（電子チケット情報）は、図４（Ａ）に示すように、チケット有効性部（「有効性」の情報）とチケット権利条項部（「権利条項」の情報）とから構成される。

【０１３７】

チケット有効性部は、図４（Ｂ）に示すように、有効性証明用秘密鍵VSK_nと付加情報とから構成される。

【０１３８】

有効性証明用秘密鍵VSK_nは、それを含む電子チケット＃ｎの有効性を証明するのに用いられる秘密鍵であり、電子チケットごとに固有の値を有する。即ち、有効性証明用秘密鍵VSK_nは、電子チケットごとに異なる。

【０１３９】

なお、有効性証明用秘密鍵VSK_nとしては、例えば、公開鍵暗号化方式による暗号を復号する秘密鍵や、電子署名を生成する秘密鍵、ゼロ知識証明可能なデータ等の、データ自体は漏らさず、その存在を示すことができるデータを採用することができる。

【０１４０】

付加情報は、例えば、電子チケットの使用回数等で構成される。なお、この使

用回数は、電子チケットの発行時には０回に設定（初期化）される。

【０１４１】

チケット権利条項部は、図４（Ｃ）に示すように、チケット権利条項TI、有効性検証用公開鍵VPK_n、発行者証明書TP_t、および条項検証用署名ASGで構成される。

【０１４２】

チケット権利条項TIは、紙によるチケットにおける記載事項に相当し、この記載事項を参照することで、電子チケットが、どのような内容の権利を行使することができるもの（どのようなサービスを受けることができるもの）であるのかを認識することができる。即ち、例えば、電子チケットが、列車の切符であるとすると、チケット権利条項TIは、例えば、乗車することのできる駅や、その乗車駅から幾ら分の区間の乗車が可能であるか、乗車可能な日等の情報から構成される。

【０１４３】

有効性検証用公開鍵VPK_nは、チケット有効性部の有効性証明用秘密鍵VSK_nに対応する公開鍵で、有効性証明用秘密鍵VSK_nの存在を検証するのに用いられる。

【０１４４】

発行者証明書TP_tは、図２で説明したように、チケット管理センタ１が、チケット発行装置３$_t$のチケット発行者に対して、あらかじめ発行する証明書で、上述したように、発行者識別情報TID_t、発行者検証用公開鍵$TSPK_t$、および発行者検証用署名TSG_tで構成される。

【０１４５】

条項検証用署名ASGは、チケット発行装置３$_t$が、チケット権利条項TI、有効性検証用公開鍵VPK_n、および発行者証明書TP_tに対し、発行者署名生成用秘密鍵$TSSK_t$（図２）を用いて生成する電子署名$D(TSSK_t, h(TI, VPK_n, TP_t))$であり、従って、条項検証用署名ASGについて、発行者証明書TP_tに含まれる発行者検証用公開鍵$TSPK_t$を用いて署名確認を行うことにより、チケット権利条項TI、有効性検証用公開鍵VPK_n、および発行者証明書TP_tの改竄の有無を確認することができる。

【０１４６】

以上のように、電子チケットが、チケット有効性部とチケット権利条項部とから構成され、チケット有効性部は、電子チケットの有効性を表すものであるから、チケット有効性部の複製を防止すれば、電子チケットの複製を防止することができることになる。従って、チケット権利条項部は、複製されても問題はなく、チケット権利条項部を構成するチケット権利条項TIには、チケットとして必要十分な情報を含ませて、自由に公開することが可能になる。さらに、チケット有効性部は、それ自体を外部に示すことなく、その存在を証明することができるものであることから、外部への漏洩や複製を防止することができ、従って、不特定の第三者に対して、「権利証明」を行うことが可能となる。

【０１４７】

次に、図５は、図４の電子チケットを発行する図１のチケット発行装置3_tの構成例を示している。

【０１４８】

チケット条項取得部１１は、電子チケットのチケット権利条項TI（図４）となる情報を取得し、チケット権利条項TIを生成して、条項検証用署名生成部１６およびチケット生成部１７に供給する。なお、チケット権利条項TIとなる情報としては、例えば、電子チケットがイベントのチケットであれば、日時、場所、イベント名、有効期限、通し番号などがある。但し、その情報の形式は自由である。

【０１４９】

ここで、電子チケットが反復使用できるものである場合、その有効期限や、使用回数の制限値は、チケット条項取得部１１において、チケット権利条項TIとなる情報として取得される。また、チケット条項取得部１１においては、例えば、図示せぬデータベースにあらかじめ登録された情報を取得するようにすることもできるし、チケット発行者が入力する情報を取得するようにすることもできる。

【０１５０】

発行者証明書取得部１２は、図２で説明したようにして、チケット管理センタ１から発行される発行者証明書TP_tを、あらかじめ取得しており、条項検証用署名生成部１６およびチケット生成部１７に供給する。

【０１５１】

発行者署名生成用秘密鍵取得部１３は、発行者署名生成用秘密鍵$TSSK_t$を取得し、条項検証用署名生成部１６に供給する。なお、発行者署名生成用秘密鍵取得部１３においては、例えば、図示せぬメモリに記憶された発行者署名生成用秘密鍵$TSSK_t$を取得するようにすることができる。

【０１５２】

乱数発生部１４は、有効性証明用秘密鍵VSK_nと有効性検証用公開鍵VPK_nを生成するための乱数を発生し、有効性鍵生成部１５に供給する。

【０１５３】

有効性鍵生成部１５は、乱数発生部１４からの乱数に基づいて、有効性証明用秘密鍵VSK_nと有効性検証用公開鍵VPK_nを生成し、チケット生成部１７に供給する。また、有効性鍵生成部１５は、有効性検証用公開鍵VPK_nを、条項検証用署名生成部１６にも供給する。なお、有効性鍵生成部１５は、電子チケット＃ｎごとに、異なる有効性証明用秘密鍵VSK_nと有効性検証用公開鍵VPK_nを生成する。

【０１５４】

条項検証用署名生成部１６は、チケット条項取得部１１からのチケット権利条項TI、発行者証明書取得部１２からの発行者証明書TP_t、および有効性鍵生成部１５からの有効性検証用公開鍵VPK_nに対して、発行者署名生成用秘密鍵取得部１３から供給される発行者署名生成用秘密鍵$TSSK_t$を用いて、条項検証用署名ASG（図４（Ｃ））となる電子署名を生成し、チケット生成部１７に供給する。

【０１５５】

チケット生成部１７は、電子チケットの付加情報（図４（Ｂ））を生成し、その付加情報と、有効性鍵生成部１５から供給される有効性証明用秘密鍵VSK_nから、電子チケットのチケット有効性部を生成する。さらに、チケット生成部１７は、チケット条項取得部１１から供給されるチケット権利条項TI、発行者証明書取得部１２から供給される発行者証明書TP_t、有効性鍵生成部１５から供給される有効性検証用公開鍵VPK_n、および条項検証用署名生成部１６から供給される条項検証用署名ASGから、電子チケットのチケット権利条項部（図４（Ｃ））を生成する。そして、チケット生成部１７は、チケット有効性部とチケット権利条項部から電子チケットを生成、発行し、チケット保持発行制御部１８に供給する。

【０１５６】

チケット保持発行制御部１８は、基本的には、後述するチケット保持装置4_uと同様の機能を有し、チケット生成部１７からの電子チケットを保持し、チケット保持装置4_uからの要求に応じて、電子チケットを、チケット保持装置4_uに譲渡するために、電子チケットを外部に出力する。

【０１５７】

なお、チケット発行装置3_tにおける発行者署名生成用秘密鍵取得部１３、乱数発生部１４、有効性鍵生成部１５、条項検証用書署名生成部１６、チケット生成部１７、およびチケット保持発行制御部１８は、耐タンパー性を有するように構成されている。

【０１５８】

次に、図６のフローチャートを参照して、図５のチケット発行装置3_tにおいて電子チケットを発行するチケット発行処理について説明する。

【０１５９】

なお、発行者証明書取得部１２においては、発行者証明書TP_tが既に取得されており、条項検証用署名生成部１６およびチケット生成部１７に供給されているものとする。さらに、発行者署名生成用秘密鍵取得部１３においても、発行者署名生成用秘密鍵$TSSK_t$が既に取得されており、条項検証用署名生成部１６に供給されているものとする。

【０１６０】

チケット発行処理では、まず最初に、ステップＳ１において、乱数発生部１４が、乱数を発生し、有効性鍵生成部１５に供給する。さらに、ステップＳ１では、有効性鍵生成部１５が、乱数発生部１４からの乱数に基づいて、有効性証明用秘密鍵VSK_nと有効性検証用公開鍵VPK_nを生成し、チケット生成部１７に供給して、ステップＳ２に進む。

【０１６１】

ステップＳ２では、チケット生成部１７が、電子チケットの付加情報を生成し、その付加情報と、有効性鍵生成部１５から供給される有効性証明用秘密鍵VSK_nから、電子チケットのチケット有効性部（図４（Ｂ））を生成する。なお、電子

チケットの使用回数が制限されている場合には、付加情報には、電子チケットの使用回数が含まれるが、この使用回数は、付加情報の生成時に０回に初期化される。

【０１６２】

その後、ステップＳ３に進み、チケット条項取得部１１が、電子チケットのチケット権利条項TIを生成し、条項検証用署名生成部１６およびチケット生成部１７に供給して、ステップＳ４に進む。ステップＳ４では、条項検証用署名生成部１６が、チケット条項取得部１１からのチケット権利条項TI、発行者証明書取得部１２からの発行者証明書TP_t、および有効性鍵生成部１５からの有効性検証用公開鍵VPK_nに対して、発行者署名生成用秘密鍵取得部１３から供給される発行者署名生成用秘密鍵$TSSK_t$を用いて、条項検証用署名ASG（図４（Ｃ））を生成し、チケット生成部１７に供給して、ステップＳ５に進む。

【０１６３】

ステップＳ５では、チケット生成部１７が、チケット条項取得部１１から供給されるチケット権利条項TI、発行者証明書取得部１２から供給される発行者証明書TP_t、有効性鍵生成部１５から供給される有効性検証用公開鍵VPK_n、および条項検証用署名生成部１６から供給される条項検証用署名ASGから、電子チケットのチケット権利条項部（図４（Ｃ））を生成し、ステップＳ６に進む。ステップＳ６では、チケット生成部１７が、ステップＳ２で生成したチケット有効性部を、例えば、共通鍵暗号化方式により暗号化する。

【０１６４】

ここで、共通鍵暗号化方式は、対称暗号化方式とも呼ばれ、データを暗号化するのに用いられる鍵と、その暗号を復号するのに用いられる鍵が同一であるもの、あるいは、異なる場合でも一方の鍵から他方の鍵を算出することが容易であるもので、具体的なアルゴリズムとしては、例えば、DES(Data Encryption Standard)、Triple DES（アメリカ合衆国商務省標準局）、FEAL(Fast data Encipherment ALgorithm)（日本電信電話株式会社）などがある。

【０１６５】

ステップＳ６においてチケット有効性部を暗号化した後は、ステップＳ７に進

み、チケット生成部１７が、暗号化されたチケット有効性部とチケット権利条項部とを組にして電子チケットを生成し、チケット保持発行制御部１８に供給する。チケット保持発行制御部１８は、ステップＳ８において、チケット生成部１７からの電子チケットを保持し、チケット発行処理を終了する。

【０１６６】

なお、チケット発行装置3_tは、図６のチケット発行処理を繰り返し行うことで、複数の電子チケットを発行する。

【０１６７】

以上のようにして、チケット保持発行制御部１８に保持された電子チケットは、チケット保持発行制御部１８において、後述するチケット譲渡処理が行われることにより、チケット保持装置4_u（のユーザ）に譲渡される。

【０１６８】

なお、電子チケットは、あらかじめ、チケット発行処理を行い、チケット保持発行制御部１８に保持しておき、チケット保持装置4_uから要求があった場合に、チケット保持発行制御部１８からチケット保持装置4_uに送信することによって譲渡することも可能であるし、チケット保持装置4_uから要求されるごとに、チケット発行処理を行って譲渡することも可能である。

【０１６９】

次に、図７は、図１のチケット保持装置4_uの構成例を示している。

【０１７０】

チケット保持装置4_uは、自身が保持している電子チケットを、他のチケット保持装置$4_{u'}$に譲渡する機能、チケット発行装置3_tや他のチケット保持装置$4_{u'}$が保持している電子チケットを譲受する機能、チケット検査装置5_sに対して、自身が保持している電子チケットの一部であるチケット権利条項部を渡し、電子チケットに基づく権利の行使を行う機能、電子チケットを破棄する機能等を有する。

【０１７１】

即ち、チケット授受制御部２１は、自身が保持している電子チケットを譲渡する場合と、他のチケット保持装置4_uから電子チケットを譲受する場合に、その

譲渡や譲受の制御を行う。さらに、チケット授受制御部２１は、後述する処理を行うにあたり、各ブロックと通信しながら、必要な制御を行う。

【０１７２】

装置証明書記憶部２２は、図３で説明したようにして、チケット管理センタ１から、あらかじめ発行された装置証明書AP_uを記憶しており、チケット授受制御部２１の制御にしたがって、記憶している装置証明書AP_uを、チケット授受制御部２１に供給する。

【０１７３】

乱数発生部２３は、チケット授受制御部２１または管理部２７の制御にしたがって、乱数を発生し、チケット授受制御部２１または管理部２７に供給する。

【０１７４】

署名処理部２４は、チケット授受制御部２１の制御にしたがい、必要に応じて、署名検証用公開鍵記憶部２５に記憶された署名検証用公開鍵P_{CA}等を用いて、電子署名に関する処理を行う。

【０１７５】

署名検証用公開鍵記憶部２５は、チケット管理センタ１が公開している署名検証用公開鍵P_{CA}をあらかじめ取得して記憶しており、その記憶している署名検証用公開鍵P_{CA}を、必要に応じて、署名処理部２４に供給する。

【０１７６】

公開鍵暗号処理部２６は、チケット管理センタ１に登録した装置検証用公開鍵APK_uに対応する装置証明用秘密鍵ASK_uを内蔵しており、チケット授受制御部２１からの制御にしたがい、必要に応じて、装置証明用秘密鍵ASK_u等を用いて、公開鍵暗号化方式による暗号化処理と復号処理を行う。

【０１７７】

管理部２７は、チケット授受制御部２１からの制御にしたがい、ストレージ部２８に保持（記憶）された電子チケットの管理を行う。即ち、管理部２７は、ストレージ部２８に記憶された電子チケットの一部であるチケット有効性部を、その複製ができないように管理し、さらに、電子チケットを他のチケット保持装置（あるいは、チケット発行装置３_t）との間でやり取りする際に、そのやり取り

の途中で、電子チケットを、その複製ができないように移動し、また、ストレージ部２８の電子チケットを譲渡した場合には、その譲渡した電子チケットを確実に削除する等の管理を行う。

【０１７８】

なお、管理部２７は、親共通鍵記憶部２７Ａを内蔵しており、親共通鍵記憶部２７Ａは、共通鍵暗号化方式での暗号化と復号に用いられる共通鍵としての親共通鍵を記憶する。

【０１７９】

ストレージ部２８は、管理部２７によって管理され、電子チケットや、その電子チケットを管理するための管理情報を記憶する。なお、ストレージ部２８は、外部から容易に着脱できないメモリやHD(Hard Disk)等で構成することも可能であるし、外部から容易に着脱できるメモリカード等で構成することも可能である。

【０１８０】

共通鍵暗号処理部２９は、管理部２７からの制御にしたがい、共通鍵暗号化方式での暗号化と復号を行う。

【０１８１】

なお、チケット保持装置4_uの装置証明書記憶部２２、乱数発生部２３、署名処理部２４、公開鍵暗号処理部２６、管理部２７、および共通鍵暗号処理部２９は、耐タンパー性を有するように構成されている。

【０１８２】

次に、図８を参照して、図７の管理部２７による、ストレージ部２８に記憶された電子チケットの管理方法について説明する。

【０１８３】

なお、図８は、ストレージ部２８に、Ｊ個の電子チケットETI_1乃至ETI_Jが記憶されている状態を示している。また、図８において影を付してある部分は、暗号化されていることを表す。

【０１８４】

管理部２７は、電子チケットETI_jを、ストレージ部２８に記憶させるが、電子

チケットETI_jを構成するチケット有効性部$ETIA_j$とチケット権利条項部$ETIB_j$のうち、チケット権利条項部$ETIB_j$については、図８（Ａ）に示すように、例えば、通常のコンピュータで扱われるファイルと同様にして、ストレージ部２８に記憶させる。

【０１８５】

また、管理部２７は、チケット有効性部$ETIA_j$については、図８（Ａ）に影を付して示すように、共通鍵暗号化方式により、電子チケットごとに異なる共通鍵で暗号化して、ストレージ部２８に記憶させる。従って、チケット有効性部$ETIA_j$は、共通鍵暗号方式により、共通鍵で暗号化された形式のファイルとして、ストレージ部２８に保存される。

【０１８６】

さらに、管理部２７は、図８（Ｂ）に示すように、チケット有効性部$ETIA_j$を、共通鍵暗号化方式により暗号化および復号する共通鍵としての子共通鍵CK_jを、管理情報として、ストレージ部２８に記憶させるが、その際、この管理情報としての子共通鍵CK_jを、管理部２７が内蔵する親共通鍵記憶部２７Ａに記憶された親共通鍵PKで共通鍵暗号化方式により暗号化する。このように、チケット有効性部$ETIA_j$の暗号化に用いられた子共通鍵CK_jも、親共通鍵PKで暗号化された形で、ストレージ部２８に記憶される。

【０１８７】

なお、電子チケットETI_jを構成するチケット有効性部$ETIA_j$とチケット権利条項部$ETIB_j$との対応関係、並びにチケット有効性部$ETIA_j$と、その暗号化および復号に用いられる子共通鍵CK_jとの対応関係は、管理情報に含められるか、あるいは、独立のファイルとして、ストレージ部２８に保存される。

【０１８８】

また、親共通鍵PKと、管理情報としての子共通鍵CK_jは、所定のタイミングで更新される。即ち、親共通鍵PKは、例えば、管理情報を構成する子共通鍵CK_jが変更されるごとに更新される。また、子共通鍵CK_jは、例えば、ストレージ部２８に記憶される電子チケットが変更されるごとに更新される。なお、更新のための新たな親共通鍵PKと子共通鍵CK_jは、例えば、後述するように、乱数に基づい

て生成される。

【０１８９】

以上のように、ストレージ部２８では、チケット有効性部$ETIA_j$が、子共通鍵CK_jで暗号化されて記憶され、さらに、その子共通鍵CK_jも親共通鍵PKで暗号化されて記憶されているので、チケット保持装置4_uに保持（記憶）されているチケット有効性部$ETIA_j$の漏洩を強固に防止することができる。

【０１９０】

次に、図９のフローチャートを参照して、図７のチケット保持装置4_uにおいて、チケット発行装置3_tまたは他のチケット保持装置$4_{u'}$から電子チケットを譲受する場合に行われるチケット譲受処理について説明する。

【０１９１】

なお、以下においては、他のチケット保持装置$4_{u'}$から電子チケットを譲受するものとして、チケット保持装置4_uによるチケット譲受処理の説明を行うが、チケット発行装置3_tから電子チケットを譲受する場合にも、チケット保持装置4_uでは、同様の処理が行われる。

【０１９２】

チケット譲受処理では、まず最初に、ステップＳ１１において、後述する譲受側の認証処理が行われ、ステップＳ１２に進む。ステップＳ１２では、チケット授受制御部２１が、ステップＳ１１における認証が成功したかどうかを判定し、成功しなかった（失敗した）と判定した場合、以降の処理をスキップして、チケット譲受処理を終了する。即ち、認証が失敗した場合には、電子チケットの譲渡を行おうとしている相手の装置である他のチケット保持装置$4_{u'}$（またはチケット発行装置3_t）が正当なものではないとして、チケット保持装置4_uは、そのような正当でない装置からの電子チケットの譲受を拒否する。

【０１９３】

一方、ステップＳ１２において、認証が成功したと判定された場合、即ち、電子チケットの譲渡を行おうとしている相手の装置である他のチケット保持装置$4_{u'}$が正当なものである場合、ステップＳ１３に進み、後述するように、正当な他のチケット保持装置$4_{u'}$は、譲渡しようとしている電子チケットのチケット

権利条項部を送信してくるので、チケット授受制御部２１は、そのチケット権利条項部を受信する。

【０１９４】

そして、ステップＳ１４に進み、チケット授受制御部２１は、ステップＳ１３で受信したチケット権利条項部の正当性を確認する、後述するチケット権利条項部の確認処理を行い、ステップＳ１５に進む。ステップＳ１５では、チケット授受制御部２１は、ステップＳ１３で受信したチケット権利条項部の正当性が確認されたかどうかを判定し、正当性を確認することができなかったと判定した場合、以降の処理をスキップして、チケット譲受処理を終了する。即ち、チケット権利条項部の正当性を確認することができなかった場合には、チケット権利条項部が改竄されているとして、チケット保持装置4_uは、そのような改竄が行われているチケット権利条項部を有する電子チケットの譲受を拒否する。

【０１９５】

一方、ステップＳ１５において、チケット権利条項部の正当性を確認することができたと判定された場合、ステップＳ１６に進み、後述するように、他のチケット保持装置$4_{u'}$は、自身の装置証明書$AP_{u'}$を送信してくるので、チケット授受制御部２１は、その装置証明書$AP_{u'}$を受信する。

【０１９６】

そして、ステップＳ１７に進み、チケット授受制御部２１は、ステップＳ１６で受信した他のチケット保持装置$4_{u'}$の装置証明書$AP_{u'}$（図３）を確認する。

【０１９７】

即ち、チケット授受制御部２１は、装置証明書$AP_{u'}$を、署名処理部２４に供給し、その装置証明書$AP_{u'}$に含まれる電子署名$ASG_{u'}$の署名確認を行わせる。

【０１９８】

この場合、署名処理部２４は、装置証明書$AP_{u'}$に含まれる電子署名$ASG_{u'}$を、署名検証用公開鍵記憶部２５に記憶されたチケット管理センタ１の署名検証用公開鍵P_{CA}で暗号化処理し、その暗号化結果と、装置証明書$AP_{u'}$に含まれる他のチケット保持装置$4_{u'}$の装置検証用公開鍵$APK_{u'}$との一致性を判定する。そして、署名処理部２４は、その一致性の判定結果を、チケット授受制御部２１に

供給する。

【０１９９】

チケット授受制御部２１は、署名処理部２４から一致性の判定結果を受信すると、ステップＳ１８に進み、その一致性の判定結果に基づき、装置証明書AP_u'が正当なものであるかどうかを判定する。ステップＳ１８において、装置証明書AP_u'が正当なものでないと判定された場合、即ち、装置証明書AP_u'に含まれる電子署名ASG_u'の、署名検証用公開鍵P_{CA}による暗号化結果と、その装置証明書AP_u'に含まれる装置検証用公開鍵APK_u'との一致性が認められない場合、以降の処理をスキップして、チケット譲受処理を終了する。即ち、この場合、電子署名ASG_uまたは装置検証用公開鍵APK_u'が改竄されているとして、チケット保持装置4_uは、そのような改竄が行われている装置証明書AP_u'を有する他のチケット保持装置$4_u'$からの電子チケットの譲受を拒否する。

【０２００】

一方、ステップＳ１８において、装置証明書AP_u'が正当なものであると判定された場合、即ち、装置証明書AP_u'に含まれる電子署名ASG_u'の、署名検証用公開鍵P_{CA}による暗号化結果と、その装置証明書AP_u'に含まれる装置検証用公開鍵APK_u'との一致性が認められた場合、ステップＳ１９に進み、チケット授受制御部２１は、乱数発生部２３を制御することにより、乱数を発生させ、その乱数から、共通鍵暗号化方式の暗号化および復号に用いる共通鍵としての暗号鍵UKを生成する。

【０２０１】

そして、ステップＳ２０に進み、チケット授受制御部２１は、その暗号鍵UKと、正当性が確認された装置証明書AP_u'に含まれる装置検証用公開鍵APK_u'を、公開鍵暗号処理部２６に供給し、公開鍵暗号処理部２６を制御することにより、暗号鍵UKを、装置検証用公開鍵APK_u'で暗号化した暗号化暗号鍵$E(APK_u', UK)$を生成させて、ステップＳ２１に進む。

【０２０２】

ステップＳ２１では、チケット授受制御部２１は、暗号化暗号鍵$E(APK_u', UK)$を、電子チケットを譲渡しようとしている他のチケット保持装置$4_u'$に送信し

、ステップＳ２２に進む。ステップＳ２２では、後述するように、暗号化暗号鍵$E(APK_u', UK)$を受信した他のチケット保持装置４$_u'$が、譲渡しようとしている電子チケットのチケット有効性部を暗号鍵UKで暗号化した暗号化チケット有効性部を送信してくるので、チケット授受制御部２１は、その暗号化チケット有効性部を受信する。

【０２０３】

そして、ステップＳ２３に進み、チケット授受制御部２１は、ステップＳ２２で暗号化チケット有効性部を正常受信することができたかどうかを判定し、できなかったと判定した場合、ステップＳ２４をスキップして、チケット譲受処理を終了する。この場合、電子チケットの譲受は失敗となる。

【０２０４】

また、ステップＳ２３において、暗号化チケット有効性部を正常受信することができたと判定された場合、ステップＳ２４に進み、ストレージ部２８に、電子チケットを追加記憶させる、後述するチケット追加処理が行われ、これにより、電子チケットの譲受に成功して、チケット授受処理を終了する。

【０２０５】

次に、図１０のフローチャートを参照して、図９のステップＳ１１における譲受側の認証処理について詳述する。

【０２０６】

譲受側の認証処理では、まず最初に、ステップＳ３１において、チケット授受制御部２１は、装置証明書記憶部２２に記憶された装置証明書AP_uを読み出し、電子チケットを譲渡しようとしている他のチケット保持装置４$_u'$に送信して、ステップＳ３２に進む。

【０２０７】

ステップＳ３２では、後述するように、装置証明書AP_uを受信した他のチケット保持装置４$_u'$が、その装置証明書AP_uに含まれる装置検証用公開鍵APK_uで乱数rを暗号化した暗号化乱数$R=E(APK_u, r)$を送信してくるので、チケット授受制御部２１は、その暗号化乱数Rを受信する。

【０２０８】

そして、ステップＳ３３に進み、チケット授受制御部２１は、暗号化乱数Rを、公開鍵暗号処理部２６に供給し、その内蔵する装置証明用秘密鍵ASK_uで復号させ、ステップＳ３４に進む。

【０２０９】

ステップＳ３４では、チケット授受制御部２１は、装置証明用秘密鍵ASK_uによる暗号化乱数Rの復号結果$r'=D(ASK_u,R)$を、他のチケット保持装置$4_{u'}$に送信し、ステップＳ３５に進む。

【０２１０】

ステップＳ３５では、後述するように、暗号化乱数Rの復号結果r'を受信した他のチケット保持装置$4_{u'}$が、その復号結果r'に基づいて、認証を行い、その認証結果を表す認証メッセージが送信されてくるので、チケット授受制御部２１は、その認証メッセージを受信し、その認証メッセージに基づいて、他のチケット保持装置$4_{u'}$における認証が成功したかどうかを判定する。

【０２１１】

ステップＳ３５において、認証が成功したと判定された場合、ステップＳ３６に進み、チケット授受制御部２１は、認証が成功したことを認識し、譲受側の認証処理を終了する。また、ステップＳ３５において、認証が成功しなかったと判定された場合、ステップＳ３７に進み、チケット授受制御部２１は、認証が失敗したことを認識して、譲受側の認証処理を終了する。

【０２１２】

なお、ステップＳ３６またはＳ３７の認識結果に基づき、図９におけるステップＳ１２の判定処理が行われることになる。

【０２１３】

次に、図１１のフローチャートを参照して、図９のステップＳ１４におけるチケット権利条項部の確認処理について詳述する。

【０２１４】

チケット権利条項部の確認処理では、まず最初に、ステップＳ４１において、チケット授受制御部２１は、電子チケットを譲渡しようとしている他のチケット保持装置$4_{u'}$から、図９のステップＳ１３において受信したチケット権利条項

部に含まれる発行者証明書TP_t（図４（Ｃ））を抽出し、ステップＳ４２に進む。ステップＳ４２では、チケット授受制御部２１は、ステップＳ４１で抽出した発行者証明書TP_tを確認する。

【０２１５】

即ち、チケット授受制御部２１は、発行者証明書TP_tを、署名処理部２４に供給し、その発行者証明書TP_tに含まれる電子署名TSG_tの署名確認を行わせる。

【０２１６】

この場合、署名処理部２４は、発行者証明書TP_tに含まれる電子署名TSG_tを、署名検証用公開鍵記憶部２５に記憶されたチケット管理センタ１の署名検証用公開鍵P_{CA}で暗号化処理し、その暗号化結果と、発行者証明書TP_tに含まれる識別情報TID_tおよび発行者検証用公開鍵$TSPK_t$の組との一致性を判定する。そして、署名処理部２４は、その一致性の判定結果を、チケット授受制御部２１に供給する。

【０２１７】

チケット授受制御部２１は、署名処理部２４から一致性の判定結果を受信すると、ステップＳ４３に進み、その一致性の判定結果に基づき、発行者証明書TP_tが正当なものであるかどうかを判定する。ステップＳ４３において、発行者証明書TP_tが正当なものでないと判定された場合、即ち、発行者証明書TP_tに含まれる電子署名TSG_tの、署名検証用公開鍵P_{CA}による暗号化結果と、その発行者証明書TP_tに含まれる識別情報TID_tおよび発行者検証用公開鍵$TSPK_t$の組との一致性が認められない場合、ステップＳ４８に進み、チケット授受制御部２１は、発行者証明書TP_tが改竄等されており、正当なものであることを確認することができなかったことを認識し、即ち、発行者証明書TP_tの正当性の確認に失敗したことを認識し、チケット権利条項部の確認処理を終了する。

【０２１８】

一方、ステップＳ４３において、発行者証明書TP_tが正当なものであると判定された場合、即ち、発行者証明書TP_tに含まれる電子署名TSG_tの、署名検証用公開鍵P_{CA}による暗号化結果と、その発行者証明書TP_tに含まれる識別情報TID_tおよび発行者検証用公開鍵$TSPK_t$の組との一致性が認められた場合、ステップＳ４

４に進み、チケット授受制御部２１は、図９のステップＳ１３において受信したチケット権利条項部（図４（Ｃ））に含まれる条項検証用署名ASGと、チケット権利条項TI、有効性検証用公開鍵VPK_n、および発行者証明書TP_tの組とを抽出するとともに、その発行者証明書TP_tに含まれる発行者検証用公開鍵$TSPK_t$を抽出し、ステップＳ４５に進む。ステップＳ４５では、チケット授受制御部２１は、ステップＳ４４で抽出した条項検証用署名ASGの署名確認を行う。

【０２１９】

即ち、チケット授受制御部２１は、ステップＳ４４で抽出した条項検証用署名ASGと、チケット権利条項TI、有効性検証用公開鍵VPK_n、および発行者証明書TP_tの組と、発行者検証用公開鍵$TSPK_t$とを、署名処理部２４に供給し、条項検証用署名ASGの署名確認を行わせる。

【０２２０】

この場合、署名処理部２４は、条項検証用署名ASGを、発行者検証用公開鍵$TSPK_t$で暗号化処理し、その暗号化結果と、チケット権利条項TI、有効性検証用公開鍵VPK_n、および発行者証明書TP_tの組との一致性を判定する。そして、署名処理部２４は、その一致性の判定結果を、チケット授受制御部２１に供給する。

【０２２１】

チケット授受制御部２１は、署名処理部２４から一致性の判定結果を受信すると、ステップＳ４６に進み、その一致性の判定結果に基づき、図９のステップＳ１３において受信したチケット権利条項部が正当なものかどうかを判定する。ステップＳ４６において、チケット権利条項部が正当なものでないと判定された場合、即ち、条項検証用署名ASGの、発行者検証用公開鍵$TSPK_t$による暗号化結果と、チケット権利条項TI、有効性検証用公開鍵VPK_n、および発行者証明書TP_tの組との一致性が認められない場合、ステップＳ４８に進み、チケット授受制御部２１は、チケット権利条項部が改竄等されており、正当なものであることを確認することができなかったことを認識し、即ち、チケット権利条項部の正当性の確認に失敗したことを認識し、チケット権利条項部の確認処理を終了する。

【０２２２】

一方、ステップＳ４６において、チケット権利条項部が正当なものであると判

定された場合、即ち、条項検証用署名ASGの、発行者検証用公開鍵$TSPK_t$による暗号化結果と、チケット権利条項TI、有効性検証用公開鍵VPK_n、および発行者証明書TP_tの組との一致性が認められる場合、ステップＳ４７に進み、チケット授受制御部２１は、チケット権利条項部が改竄等されていない、正当なものであることを確認することができたことを認識し、即ち、チケット権利条項部の正当性の確認に成功したことを認識し、チケット権利条項部の確認処理を終了する。

【０２２３】

なお、ステップＳ４７またはＳ４８の認識結果に基づき、図９におけるステップＳ１５の判定処理が行われることになる。

【０２２４】

次に、図１２のフローチャートを参照して、図９のステップＳ２４におけるチケット追加処理について詳述する。

【０２２５】

チケット追加処理では、まず最初に、ステップＳ５１において、チケット授受制御部２１は、管理部２７を制御することにより、他のチケット保持装置$４_{u'}$から、図９のステップＳ１３で受信したチケット権利条項部と、ステップＳ２２で受信した暗号化チケット有効性部とを、ストレージ部２８に追加記憶させ、ステップＳ５２に進む。

【０２２６】

ステップＳ５２では、管理部２７が、ストレージ部２８に記憶されている、暗号化された管理情報としての子共通鍵CK_jを読み出すとともに、親共通鍵記憶部２７Ａに記憶されている親共通鍵PKを読み出し、共通鍵記憶部２９に供給して、暗号化されている子共通鍵CK_jを、親共通鍵PKで復号させる。

【０２２７】

そして、ステップＳ５３に進み、管理部２７は、図９のステップＳ１９で生成された暗号鍵UKを、チケット授受制御部２１から取得し、その暗号鍵UKを、ステップＳ５２でストレージ部２８から読み出した管理情報に、新たな子共通鍵として追加して、ステップＳ５４に進む。

【０２２８】

ステップＳ５４では、管理部２７は、乱数発生部２３に乱数を発生させ、その乱数から、新たな親共通鍵PKを生成して、親共通鍵記憶部２７の記憶内容を、その新たな親共通鍵PKで更新する（親共通鍵記憶部２７に、新たな親共通鍵PKを上書きする）。

【０２２９】

そして、ステップＳ５５に進み、管理部２７は、新たな親共通鍵PKと、暗号鍵UKを新たな子共通鍵として追加した管理情報（以下、適宜、新たな管理情報という）とを、共通鍵暗号処理部２９に供給し、新たな管理情報を、新たな親共通鍵PKで暗号化させる。さらに、管理部２７は、ステップＳ５５において、その暗号化された新たな管理情報を、ストレージ部２８に上書きする形で記憶させ、チケット追加処理を終了する。

【０２３０】

なお、ステップＳ５１においてストレージ部２８に記憶される暗号化チケット有効性部は、後述するように、電子チケットを譲渡した他のチケット保持装置$4_{u'}$において、新たな子共通鍵として管理情報に追加される暗号鍵UKで、チケット有効性部が暗号化されたものであり、電子チケットを譲受するチケット保持装置4_{u}では、ストレージ部２８に記憶させる前に、特に処理する必要はない。

【０２３１】

次に、図１３のフローチャートを参照して、図５のチケット発行装置3_{t}または図７のチケット保持装置4_{u}において、他のチケット保持装置$4_{u'}$に電子チケットを譲渡する場合に行われるチケット譲渡処理について説明する。

【０２３２】

なお、以下においては、チケット保持装置4_{u}から電子チケットを譲渡するものとして、チケット譲渡処理の説明を行うが、チケット発行装置3_{t}から電子チケットを譲渡する場合にも、チケット発行装置3_{t}のチケット保持発行制御部１８において、同様の処理が行われる。

【０２３３】

ここで、チケット譲渡処理には、図３で説明した装置証明用秘密鍵ASK_{u}、装置検証用公開鍵APK_{u}、およびチケット管理センタ１が発行する装置証明書AP_{u}が必

要であり、従って、チケット発行装置３_tのチケット保持発行制御部１８がチケット譲渡処理を行うには、これらの装置証明用秘密鍵ASK_t、装置検証用公開鍵APK_t、および装置証明書AP_tを有している必要がある。

【０２３４】

チケット譲渡処理では、まず最初に、ステップＳ６１において、後述する譲渡側の認証処理が行われ、ステップＳ６２に進む。ステップＳ６２では、チケット授受制御部２１が、ステップＳ６１における認証が成功したかどうかを判定し、成功しなかった（失敗した）と判定した場合、以降の処理をスキップして、チケット譲渡処理を終了する。即ち、認証が失敗した場合には、電子チケットの譲渡相手の装置である他のチケット保持装置$４_{u'}$が正当なものではないとして、チケット保持装置４_uは、そのような正当でない装置への電子チケットの譲渡を拒否する。

【０２３５】

一方、ステップＳ６２において、認証が成功したと判定された場合、即ち、電子チケットの譲渡相手の装置である他のチケット保持装置$４_{u'}$が正当なものである場合、ステップＳ６３に進み、チケット授受制御部２１は、管理部２７を制御することにより、ストレージ部２８から、譲渡しようとしている電子チケットのチケット条項部を読み出させ、譲渡相手である他のチケット保持装置$４_{u'}$に送信して、ステップＳ６４に進む。

【０２３６】

ステップＳ６４では、チケット授受制御部２１は、装置証明書記憶部２２に記憶された装置証明書AP_uを読み出し、譲渡相手である他のチケット保持装置$４_{u'}$に送信する。

【０２３７】

譲渡相手である他のチケット保持装置$４_{u'}$では、上述のチケット譲受処理（図９）が行われ、ステップＳ６３で送信したチケット権利条項部と、ステップＳ６４で送信した装置証明書AP_uの正当性が確認されると、チケット譲受処理のステップＳ２１で、暗号化暗号鍵$E(APK_u,UK)$を送信してくるので、チケット授受制御部２１は、ステップＳ６５において、その暗号化暗号鍵$E(APK_u,UK)$を受信する

【０２３８】

そして、ステップＳ６６に進み、チケット授受制御部２１は、ステップＳ６５で受信した暗号化暗号鍵E(APK$_u$,UK)を復号する。

【０２３９】

即ち、暗号化暗号鍵E(APK$_u$,UK)は、ステップＳ６４において、譲渡相手である他のチケット保持装置４$_u$'に対して送信した装置証明書AP$_u$に含まれる装置検証用公開鍵APK$_u$を用いて、譲渡相手である他のチケット保持装置４$_u$'が、暗号鍵UKを暗号化したものであり、従って、公開鍵暗号処理部２６が内蔵する装置証明用秘密鍵ASK$_u$で復号することができる。

【０２４０】

そこで、ステップＳ６６では、チケット授受制御部２１は、暗号化暗号鍵E(APK$_u$,UK)を、公開鍵暗号処理部２６に供給し、装置証明用秘密鍵ASK$_u$を用いて、暗号鍵UKに復号させる。

【０２４１】

チケット授受制御部２１は、以上のようにして、暗号鍵UKを得た後、ステップＳ６６からステップＳ６７に進み、管理部２７を制御することにより、ストレージ部２８に記憶された、譲渡しようとしてる電子チケットの暗号化チケット有効性部を復号させる。

【０２４２】

即ち、この場合、管理部２７は、親共通鍵記憶部２７Ａに記憶された親共通鍵PKを読み出すとともに、ストレージ部２８に記憶された暗号化された管理情報（以下、適宜、暗号化管理情報という）を読み出し、共通鍵暗号処理部２９に供給する。共通鍵暗号処理部２９は、暗号化管理情報を、親共通鍵PKを用いて、管理情報に復号し、その管理情報から、譲渡しようとしてる電子チケットのチケット有効性部の暗号化に用いた子共通鍵CK$_j$を抽出する。

【０２４３】

その後、管理部２７は、ストレージ部２８から、譲渡しようとしてる電子チケットの暗号化チケット有効性部を読み出し、共通鍵暗号処理部２９に供給する。

共通鍵暗号処理部２９は、暗号化チケット有効性部を、管理情報から抽出した子共通鍵CK_iを用いて、チケット有効性部に復号する。

【０２４４】

共通鍵暗号処理部２９において、以上のようにして、チケット有効性部が復号されると、ステップＳ６８に進み、チケット授受制御部２１は、ステップＳ６６で復号した暗号鍵UKを、管理部２７に供給し、その暗号鍵UKによるチケット有効性部の暗号化を要求する。この場合、管理部２７は、暗号鍵UKを、共通鍵暗号処理部２９に供給し、その暗号鍵UKを用いて、ステップＳ６７で復号したチケット有効性部を暗号化させる。

【０２４５】

共通鍵暗号処理部２９において、暗号鍵UKによるチケット有効性部の暗号化が行われることにより得られる暗号化チケット有効性部は、管理部２７を介して、チケット授受制御部２１に供給される。チケット授受制御部２１は、ステップＳ６９において、その暗号化チケット有効性部を、譲渡相手である他のチケット保持装置$4_{u'}$に対して送信し、ステップＳ７０に進む。

【０２４６】

ステップＳ７０では、ストレージ部２８から、譲渡した電子チケットを削除する、後述するチケット削除処理が行われ、チケット譲渡処理を終了する。

【０２４７】

次に、図１４のフローチャートを参照して、図１３のステップＳ６１における譲渡側の認証処理について詳述する。

【０２４８】

譲渡側の認証処理では、まず最初に、ステップＳ８１において、チケット授受制御部２１は、譲渡相手である（電子チケットを譲受する）他のチケット保持装置$4_{u'}$が、譲受側の認証処理（図１０）のステップＳ３１で送信してくる装置証明書$AP_{u'}$（図３）を受信し、ステップＳ８２に進む。

【０２４９】

ステップＳ８２では、チケット授受制御部２１は、ステップＳ８１で受信した他のチケット保持装置$4_{u'}$の装置証明書$AP_{u'}$を確認する。

【０２５０】

即ち、チケット授受制御部２１は、装置証明書AP_u，を、署名処理部２４に供給し、その装置証明書AP_u，に含まれる電子署名ASG_u，の署名確認を行わせる。

【０２５１】

この場合、署名処理部２４は、装置証明書AP_u，に含まれる電子署名ASG_u，を、署名検証用公開鍵記憶部２５に記憶されたチケット管理センタ１の署名検証用公開鍵P_{CA}で暗号化処理し、その暗号化結果と、装置証明書AP_u，に含まれる他のチケット保持装置4_u，の装置検証用公開鍵APK_u，との一致性を判定する。そして、署名処理部２４は、その一致性の判定結果を、チケット授受制御部２１に供給する。

【０２５２】

チケット授受制御部２１は、署名処理部２４から一致性の判定結果を受信すると、ステップＳ８３に進み、その一致性の判定結果に基づき、装置証明書AP_u，が正当なものであるかどうかを判定する。ステップＳ８３において、装置証明書AP_u，が正当なものでないと判定された場合、即ち、装置証明書AP_u，に含まれる電子署名ASG_u，の、署名検証用公開鍵P_{CA}による暗号化結果と、その装置証明書AP_u，に含まれる装置検証用公開鍵APK_u，との一致性が認められない場合、ステップＳ９０に進み、認証が失敗したことを認識するとともに、その旨の認証メッセージを、譲渡相手の他のチケット保持装置4_u，に送信して、譲渡側の認証処理を終了する。

【０２５３】

一方、ステップＳ８３において、装置証明書AP_u，が正当なものであると判定された場合、即ち、装置証明書AP_u，に含まれる電子署名ASG_u，の、署名検証用公開鍵P_{CA}による暗号化結果と、その装置証明書AP_u，に含まれる装置検証用公開鍵APK_u，との一致性が認められた場合、ステップＳ８４に進み、チケット授受制御部２１は、乱数発生部２３を制御することにより、乱数rを発生させ、ステップＳ８５に進む。

【０２５４】

ステップＳ８５では、チケット授受制御部２１は、正当なものであることが確

認された装置証明書$AP_{u'}$に含まれる装置検証用公開鍵$APK_{u'}$を抽出し、乱数rとともに、公開鍵暗号処理部２６に供給することで、乱数rを、装置検証用公開鍵$APK_{u'}$で暗号化させる。

【０２５５】

そして、ステップＳ８６に進み、チケット授受制御部２１は、公開鍵暗号処理部２６において、装置検証用公開鍵$APK_{u'}$による乱数rの暗号化が行われることにより得られた暗号化乱数$R=E(APK_{u'},r)$を、譲渡相手の他のチケット保持装置$4_{u'}$に送信し、ステップＳ８７に進む。

【０２５６】

暗号化乱数$R=E(APK_{u'},r)$を受信した他のチケット保持装置$4_{u'}$では、上述の譲受側の認証処理（図１０）のステップＳ３３において、暗号化乱数$R=E(APK_{u'},r)$を、装置証明用秘密鍵$ASK_{u'}$で復号し、さらに、ステップＳ３４において、その暗号化乱数Rの復号結果$r'=D(ASK_{u'},R)$を送信してくるので、ステップＳ８７では、チケット授受制御部２１が、その復号結果$r'=D(ASK_{u'},R)$を受信し、ステップＳ８８に進む。

【０２５７】

ステップＳ８８では、チケット授受制御部２１は、ステップＳ８４で発生した乱数rと、ステップＳ８７で受信した暗号化乱数Rの復号結果r'とが一致するかどうかを判定する。ステップＳ８８において、乱数rと、暗号化乱数Rの復号結果r'とが一致しないと判定された場合、ステップＳ９０に進み、チケット授受制御部２１は、譲渡相手の他のチケット保持装置$4_{u'}$が、チケット管理センタ１に登録されていない装置（正当でない装置）であるとして、認証が失敗したことを認識し、さらに、その旨の認証メッセージを、譲渡相手の他のチケット保持装置$4_{u'}$に送信して、譲渡側の認証処理を終了する。

【０２５８】

一方、ステップＳ８８において、乱数rと、暗号化乱数Rの復号結果r'とが一致すると判定された場合、ステップＳ８９に進み、チケット授受制御部２１は、譲渡相手の他のチケット保持装置$4_{u'}$が、チケット管理センタ１に登録されていいる正当な装置であるとして、認証が成功したことを認識し、さらに、その旨の

認証メッセージを、譲渡相手の他のチケット保持装置$4_{u'}$に送信して、譲渡側の認証処理を終了する。

【０２５９】

なお、ステップＳ８９またはＳ９０の認識結果に基づき、図１３におけるステップＳ６２の判定処理が行われることになる。

【０２６０】

次に、図１５のフローチャートを参照して、図１３のステップＳ７０におけるチケット削除処理について詳述する。

【０２６１】

チケット削除処理では、まず最初に、ステップＳ１０１において、管理部２７は、ストレージ部２８に記憶されている暗号化管理情報を読み出すとともに、親共通鍵記憶部２７Ａに記憶されている親共通鍵PKを読み出し、共通鍵記憶部２９に供給して、暗号化管理情報を、親共通鍵PKを用いて、管理情報に復号させる。

【０２６２】

そして、ステップＳ１０２に進み、管理部２７は、削除対象の電子チケットのチケット有効性部の暗号化に用いた子共通鍵CK_jを、ステップＳ１０１で復号された管理情報から削除し、ステップＳ１０３に進む。

【０２６３】

ここで、削除対象の電子チケットとは、電子チケットの譲渡が行われた場合には、その譲渡された電子チケットを意味する。

【０２６４】

ステップＳ１０３では、管理部２７は、乱数発生部２３に乱数を発生させ、その乱数から、新たな親共通鍵PKを生成して、親共通鍵記憶部２７の記憶内容を、その新たな親共通鍵PKで更新する（親共通鍵記憶部２７に、新たな親共通鍵PKを上書きする）。

【０２６５】

そして、ステップＳ１０４に進み、管理部２７は、ステップＳ１０２で、削除対象の電子チケットのチケット有効性部の暗号化に用いた子共通鍵CK_jを削除した管理情報と、ステップＳ１０３で得られた新たな親共通鍵PKを、共通鍵暗号処

理部２９に供給し、その管理情報を、新たな親共通鍵PKで暗号化させることにより、新たな暗号化管理情報を得る。さらに、ステップＳ１０４において、管理部２７は、その新たな暗号化管理情報を、ストレージ部２８に上書きする形で記憶させ、ステップＳ１０５に進む。

【０２６６】

ステップＳ１０５では、管理部２７は、ストレージ部２８から、削除対象の電子チケットを構成する暗号化チケット有効性部とチケット権利条項部を削除し、チケット削除処理を終了する。

【０２６７】

なお、図１５のチケット削除処理は、電子チケットが譲渡された場合に、その電子チケットを削除対象として行われる他、電子チケットのチケット権利条項部の記述、あるいは暗黙の仮定によって、電子チケットの有効期間や、使用回数の制限値を越えた場合、さらには、所有者の意志により、不要となった電子チケットが存在する場合等に、その電子チケットを削除対象として行われる。

【０２６８】

次に、図１６のフローチャートを参照して、図７のチケット保持装置4_uにおいて、チケット検査装置5_sに対して、電子チケットに基づく権利を行使または証明する場合に行われるチケットの権利行使／証明処理について説明する。

【０２６９】

なお、説明の便宜上、使用回数が制限された電子チケットに基づく権利を行使する際に、使用回数も含めて、電子チケットの権利を証明し、その結果として、使用回数が１回増加する場合を、以下、適宜、権利行使という。また、電子チケットの有効性だけを示す場合、および使用回数の制限のない電子チケット（有効期限や日付の指定は、あってもかまわない）に基づく権利を行使する場合のように、電子チケットを所有していることを示す場合を、以下、適宜、権利証明という。

【０２７０】

従って、例えば、電子チケットが回数券で、その回数券によって、改札を通る場合等が、権利行使に該当する。また、電子チケットが定期券で、その定期券に

よって、改札を通る場合や、新幹線の車内において、乗車券や特急券としての電子チケットを見せる場合等が、権利証明に該当する。なお、電子チケットの譲渡が行われる場合に、受け取ろうとしている電子チケットや、受け取った電子チケットの有効性の確認を行うことも、権利証明に該当する。

【０２７１】

チケットの権利行使／証明処理では、まず最初に、例えば、ユーザが、チケット保持装置4_uのストレージ部２８に保持（記憶）されている電子チケットのうち、権利を行使または証明しようとしている電子チケットを選択する。ここで、このようにして選択された電子チケットを、以下、適宜、注目電子チケットという。

【０２７２】

そして、ステップＳ１１１において、チケット授受制御部２１は、管理部２７を制御することにより、注目電子チケットのチケット権利条項部を、ストレージ部２８から読み出させる。さらに、ステップＳ１１１では、チケット授受制御部２１は、ストレージ部２８から読み出されたチケット権利条項部を、チケット検査装置5_sに送信し、ステップＳ１１２に進む。

【０２７３】

ステップＳ１１２では、後述するように、チケット保持装置4_uからチケット権利条項部を受信したチケット検査装置5_sが、乱数rを送信してくるので、チケット授受制御部２１は、その乱数rを受信し、ステップＳ１１３に進む。

【０２７４】

ステップＳ１１３では、管理部２７は、ストレージ部２８に記憶されている暗号化管理情報を読み出すとともに、親共通鍵記憶部２７Ａに記憶されている親共通鍵PKを読み出し、共通鍵記憶部２９に供給して、暗号化管理情報を、親共通鍵PKを用いて、管理情報に復号させる。

【０２７５】

そして、ステップＳ１１４に進み、管理部２７は、復号された管理情報から、注目電子チケットのチケット有効性部の暗号化に用いた子共通鍵CK_jを抽出し、ステップＳ１１５に進む。ステップＳ１１５では、管理部２７は、ストレージ部

２８から、注目電子チケットの暗号化チケット有効性部を読み出し、ステップＳ１１４で得た子共通鍵CK_jとともに、共通鍵暗号処理部２９に供給して、暗号化チケット有効性部を復号させる。

【０２７６】

即ち、この場合、共通鍵暗号処理部２９は、暗号化チケット有効性部を、子共通鍵CK_jで、チケット有効性部に復号し、管理部２７を介して、チケット授受制御部２１に供給する。

【０２７７】

その後、チケット授受制御部２１は、ステップＳ１１６に進み、ステップＳ１１１でチケット検査装置5_sに送信した注目電子チケットのチケット権利条項部（図４（Ｃ））におけるチケット権利条項TIを参照することにより、注目電子チケットに基づく権利が、使用回数の制限されているもの（以下、適宜、回数制限付きの権利という）であるかどうかを判定する。

【０２７８】

ステップＳ１１６において、注目電子チケットに基づく権利が、回数制限付きの権利でないと判定された場合、ステップＳ１１７に進み、チケット授受制御部２１は、ステップＳ１１２でチケット検査装置5_sから受信した乱数rと、ステップＳ１１５で得た注目電子チケットのチケット有効性部（図４（Ｂ））に含まれる有効性証明用秘密鍵VSK_nを、署名処理部２４に供給し、乱数rに対する電子署名SG(r)を生成させる。

【０２７９】

即ち、この場合、署名処理部２４は、有効性証明用秘密鍵VSK_nを用いて、乱数rの一方向性関数値h(r)を復号処理することにより、乱数rに対する電子署名$SG(r)=D(VSK_n,h(r))$を生成し、この電子署名SG(r)を、注目電子チケットの有効性を表す有効性証明用秘密鍵VSK_nの存在を証明する権利証明用署名として、チケット授受制御部２１に供給する。

【０２８０】

チケット授受制御部２１は、署名処理部２４から、権利証明用署名SG(r)を受信すると、ステップＳ１１８に進み、その権利証明用署名SG(r)を、チケット検

査装置５$_s$に送信し、ステップＳ１２５に進む。

【０２８１】

一方、ステップＳ１１６において、注目電子チケットに基づく権利が、回数制限付きの権利であると判定された場合、ステップＳ１１９に進み、電子チケットの権利証明を行うのかどうかが判定される。なお、この判定は、例えば、ユーザによるチケット保持装置４$_u$の操作に基づいて行われる。

【０２８２】

ステップＳ１１９において、権利証明を行うと判定された場合、即ち、例えば、注目電子チケットが、列車の乗車券であり、列車の中で、乗車券を所有していることの確認のために、その乗車券を、車掌に提示しようとしている場合、ステップＳ１２０に進み、チケット授受制御部２１は、ステップＳ１１２でチケット検査装置５$_s$から受信した乱数rと、ステップＳ１１５で得た注目電子チケットのチケット有効性部（図４（Ｂ））に含まれる有効性証明用秘密鍵VSK_nおよび付加情報を、署名処理部２４に供給し、乱数rと付加情報に含まれる使用回数cに対する電子署名SG(r,c)を生成させる。

【０２８３】

即ち、この場合、署名処理部２４は、有効性証明用秘密鍵VSK_nを用いて、乱数rと付加情報に含まれる使用回数cの一方向性関数値h(r,c)を復号処理することにより、乱数rと使用回数cに対する電子署名$SG(r,c)=D(VSK_n,h(r,c))$を生成し、この電子署名SG(r,c)を、注目電子チケットの有効性を表す有効性証明用秘密鍵VSK_nの存在を証明する権利証明用署名として、チケット授受制御部２１に供給する。

【０２８４】

チケット授受制御部２１は、署名処理部２４から、権利証明用署名SG(r,c)を受信すると、ステップＳ１２１に進み、その権利証明用署名SG(r)を、チケット有効性部の付加情報に含まれる使用回数cとともに、チケット検査装置５$_s$に送信し、ステップＳ１２５に進む。

【０２８５】

一方、ステップＳ１１９において、電子チケットの権利証明を行うのではない

と判定された場合、即ち、電子チケットの権利行使が行われる場合（例えば、注目電子チケットが、列車の１回限りの乗車券や回数券であり、列車に乗車するために、ユーザが改札を通ろうとしている場合）、ステップＳ１２２に進み、チケット授受制御部２１は、ステップＳ１１２でチケット検査装置5_sから受信した乱数rと、ステップＳ１１５で得た注目電子チケットのチケット有効性部（図４（Ｂ））に含まれる有効性証明用秘密鍵VSK_nおよび付加情報を、署名処理部２４に供給するとともに、権利行使を行うことを表す行使コードeを、署名処理部２４に供給する。なお、行使コードeは、例えば、チケット保持装置4_uとチケット検査装置5_sとの間で、あらかじめ定められているものとする。

【０２８６】

さらに、ステップＳ１２２において、チケット授受制御部２１は、署名処理部２４に、乱数r、付加情報に含まれる使用回数c、および行使コードeに対する電子署名SG(r,c,e)を生成させる。

【０２８７】

即ち、この場合、署名処理部２４は、有効性証明用秘密鍵VSK_nを用いて、乱数r、付加情報に含まれる使用回数c、および行使コードeの一方向性関数値h(r,c,e)を復号処理することにより、乱数r、使用回数c、および行使コードeに対する電子署名$SG(r,c,e)=D(VSK_n,h(r,c,e))$を生成し、この電子署名SG(r,c,e)を、注目電子チケットの有効性を表す有効性証明用秘密鍵VSK_nの存在を証明する権利証明用署名として、チケット授受制御部２１に供給する。

【０２８８】

チケット授受制御部２１は、署名処理部２４から、権利証明用署名SG(r,c,e)を受信すると、ステップＳ１２３に進み、その権利証明用署名SG(r,c,e)を、チケット有効性部の付加情報に含まれる使用回数cとともに、チケット検査装置5_sに送信し、ステップＳ１２４に進む。

【０２８９】

ステップＳ１２４では、チケット授受制御部２１は、注目電子チケットにおけるチケット有効性部の付加情報に含まれる使用回数cを１だけインクリメントし、ステップＳ１２５に進む。

【０２９０】

ステップＳ１２５では、管理部２７は、ステップＳ１１４で管理情報から抽出した、注目電子チケットのチケット有効性部の暗号化に用いられていた子共通鍵CK_jを更新する。即ち、管理部２７は、乱数発生部２３に乱数を発生させ、その乱数から、新たな子共通鍵CK'_jを生成して、管理情報における元の子共通鍵CK_jに上書きすることにより、新たな管理情報を得る。

【０２９１】

そして、ステップＳ１２６に進み、管理部２７は、チケット授受制御部２１から、注目電子チケットのチケット有効性部（このチケット有効性部の付加情報に含まれる使用回数cは、ステップＳ１２２で更新されている場合がある）を取得し、そのチケット有効性部を、新たな子共通鍵CK'_jとともに、共通鍵暗号処理部２９に供給して暗号化させる。即ち、この場合、共通鍵暗号処理部２９は、注目電子チケットのチケット有効性部２９を、新たな子共通鍵CK'_jで暗号化し、その結果得られる暗号化チケット有効性部を、管理部２７に供給する。

【０２９２】

ステップＳ１２６では、さらに、管理部２７が、共通鍵暗号処理部２９から供給される暗号化チケット有効性部を、ストレージ部２８の注目電子チケットの暗号化チケット有効性部に上書きし、ステップＳ１２７に進む。

【０２９３】

ステップＳ１２７では、管理部２７は、乱数発生部２３に乱数を発生させ、その乱数から、新たな親共通鍵PKを生成して、親共通鍵記憶部２７の記憶内容を、その新たな親共通鍵PKで更新する（親共通鍵記憶部２７に、新たな親共通鍵PKを上書きする）。

【０２９４】

そして、ステップＳ１２８に進み、管理部２７は、新たな親共通鍵PKと、ステップＳ１２５で得た新たな管理情報とを、共通鍵暗号処理部２９に供給し、その新たな管理情報を、新たな親共通鍵PKで暗号化させる。さらに、ステップＳ１２８では、管理部２７は、その暗号化された新たな管理情報を、ストレージ部２８に上書きする形で記憶させ、チケットの権利行使／証明処理を終了する。

【０２９５】

次に、図１７は、図１のチケット検査装置５$_s$の構成例を示している。

【０２９６】

チケット検査装置５$_s$は、電子チケットに基づく権利が行使される際や、その権利の行使中に、サービス提供者が、その電子チケットを検査するための機能を有する。具体的には、チケット検査装置５$_s$は、チケット保持装置４$_u$から、電子チケットの一部であるチケット権利条項部を受け取り、その正当性を確認する機能を有する。さらに、チケット検査装置５$_s$は、チケット保持装置４$_u$がチケット有効性部を保持していることを、チャレンジアンドレスポンスの認証方法によって確認する機能を有する。

【０２９７】

なお、チケット検査装置５$_s$は、上述のように、電子チケットを検査する機能を有することから、ユーザが、他のユーザ等から電子チケットを譲受する際に、その譲受前または譲受後の電子チケットが有効であるかどうかの確認に用いることも可能である。従って、以下説明するチケット検査装置５$_s$は、それ自体単独で使用する他、チケット保持装置４$_u$に内蔵させて使用することも可能である。

【０２９８】

チケット検査制御部３１は、チケット保持装置４$_u$が保持している電子チケットを検査する、後述するチケット検査処理を行うにあたり、各ブロックと通信しながら、必要な制御を行う。

【０２９９】

乱数発生部３２は、チケット検査制御部３１の制御にしたがって、乱数を発生し、チケット検査制御部３１に供給する。

【０３００】

検査内容記憶部３３には、チケット検査装置５$_s$を有するサービス提供者がサービスの提供のために必要な条件（以下、適宜、サービス条件という）を記憶させる。ここで、例えば、サービス提供者がイベント開催のサービスを提供し、チケット検査装置５$_s$が、イベント会場への入場をチェックするものであるとすれば、開催日時や、場所、イベント名等が、サービス条件に該当する。なお、チケ

ット検査装置５$_s$の用途等に応じて、検査内容記憶部３３は省略可能である。検査内容記憶部３３が設けられていない場合は、サービス条件が設定されていないものとして扱われる。

【０３０１】

署名処理部３４は、チケット検査制御部３１の制御にしたがい、必要に応じて、署名検証用公開鍵記憶部３５に記憶された署名検証用公開鍵P_{CA}等を用いて、電子署名に関する処理を行う。

【０３０２】

署名検証用公開鍵記憶部３５は、チケット管理センタ１が公開している署名検証用公開鍵P_{CA}をあらかじめ取得して記憶しており、その記憶している署名検証用公開鍵P_{CA}を、必要に応じて、署名処理部３４に供給する。

【０３０３】

表示部３６は、チケット検査制御部３１の制御にしたがって、検査する電子チケットの有効性や内容等を表示する。なお、表示部３６も、検査内容記憶部３３と同様に、チケット検査装置５$_s$の用途等に応じて、省略可能である。

【０３０４】

次に、図１８のフローチャートを参照して、図１７のチケット検査装置５$_s$において、チケット保持装置４$_u$が保持している電子チケットを検査する場合に行われるチケット検査処理について説明する。

【０３０５】

チケット検査処理では、まず最初に、ステップＳ１３１において、チケット検査制御部３１は、チケット保持装置４$_u$がチケットの権利行使／証明処理（図１６）を行うことにより、ステップＳ１１１で送信してくる注目電子チケットのチケット権利条項部を受信し、ステップＳ１３２に進む。

【０３０６】

ステップＳ１３２では、チケット検査制御部３１は、ステップＳ１３１で受信したチケット権利条項部の正当性を確認する、図１１で説明したチケット権利条項部の確認処理を行い、ステップＳ１３３に進む。

【０３０７】

ステップＳ１３３では、チケット検査制御部３１は、ステップＳ１３１で受信したチケット権利条項部の正当性が確認されたかどうかを判定し、正当性を確認することができなかったと判定した場合、ステップＳ１４７に進み、チケット検査制御部３１は、チケット権利条項部が改竄等されていることにより、チケット権利条項部の正当性を確認することができなかったとして、サービスを提供することができないこと（サービス提供不可）を認識し、チケット検査処理を終了する。

【０３０８】

この場合、チケット保持装置4_uのユーザは、サービス提供者からサービスの提供を受けることができない。即ち、例えば、チケット検査装置5_sが列車に乗車するための改札である場合には、チケット保持装置4_uのユーザは、その入場を拒否される。

【０３０９】

一方、ステップＳ１３３において、チケット権利条項部の正当性を確認することができたと判定された場合、ステップＳ１３４に進み、チケット検査制御部３１は、正当性が確認されたチケット権利条項部（図４（Ｃ））におけるチケット権利条項TIが、検査内容記憶部３３に記憶されているサービス条件を満足する（サービス条件に合致する）かどうかを判定する。なお、チケット検査装置5_sが、例えば、チケット保持装置4_uに内蔵され、電子チケットを譲受する際に、その電子チケットの有効性の検査に用いられる場合には、ステップＳ１３４の処理はスキップされ、ステップＳ１３５に進む。

【０３１０】

ステップＳ１３４において、チケット権利条項部におけるチケット権利条項TIがサービス条件を満足しないと判定された場合、即ち、例えば、チケット検査装置5_sが列車に乗車するための改札であるのに対して、ステップＳ１３１で受信したチケット権利条項部を有する電子チケットがイベントの入場券である場合、ステップＳ１４７に進み、チケット検査制御部３１は、サービスを提供することができないことを認識し、チケット検査処理を終了する。

【０３１１】

この場合も、チケット保持装置４$_u$のユーザは、サービス提供者からサービスの提供を受けることができない。

【０３１２】

一方、ステップＳ１３４において、チケット権利条項部におけるチケット権利条項TIがサービス条件を満足すると判定された場合、ステップＳ１３５に進み、チケット検査制御部３１は、乱数発生部３２を制御することにより、チャレンジアンドレスポンスの方法による認証を行うための乱数rを発生させ、ステップＳ１３６に進む。ステップＳ１３６では、チケット検査制御部３１は、ステップＳ１３５で得た乱数rを、チケット保持装置４$_u$に送信し、ステップＳ１３７に進む。

【０３１３】

ステップＳ１３７では、チケット検査制御部３１は、ステップＳ１３１で受信した注目電子チケットのチケット権利条項部におけるチケット権利条項TIを参照することにより、注目電子チケットに基づく権利が、使用回数の制限されているもの、即ち、回数制限付きの権利であるかどうかを判定する。

【０３１４】

ステップＳ１３７において、注目電子チケットに基づく権利が、回数制限付きの権利でないと判定された場合、ステップＳ１３８に進み、チケット検査制御部３１は、チケット保持装置４$_u$が、上述のチケットの権利行使／証明処理（図１６）を行うことによって、ステップＳ１１８で送信してくる権利証明用署名SG(r)を受信する。

【０３１５】

そして、ステップＳ１３９に進み、チケット検査制御部３１は、ステップＳ１３８で受信した権利証明用署名SG(r)の署名確認を行う。

【０３１６】

即ち、チケット検査制御部３１は、正当性の確認されたチケット権利条項部（図４（Ｃ））から、有効性検証用公開鍵VPK_nを抽出し、権利証明用署名SG(r)とともに、署名処理部３４に供給して、権利証明用署名SG(r)の署名確認を行わせる。

【０３１７】

この場合、署名処理部３４は、権利証明用署名SG(r)を、有効性検証用公開鍵VPK_nで暗号化処理し、その暗号化結果と、ステップＳ１３６で得た乱数rとの一致性を判定する。そして、署名処理部３４は、その一致性の判定結果を、チケット検査制御部３１に供給する。

【０３１８】

ここで、権利証明用署名SG(r)は、チケット保持装置4_uが、上述のチケットの権利行使／証明処理（図１６）を行うことにより、ステップＳ１１７において、有効性証明用秘密鍵VSK_nを用いて、乱数rの一方向性関数値h(r)を復号処理して得られるものであるから、チケット保持装置4_uおよび注目電子チケットが正当なものであれば、権利証明用署名$SG(r)=D(VSK_n,h(r))$を、有効性検証用公開鍵VPK_nで暗号化処理した暗号化結果$E(VPK_n,SG(r))$と、乱数rの一方向性関数値h(r)とは一致し、署名処理部３４では、一致性があると判定されることになる。

【０３１９】

チケット検査制御部３１は、署名処理部３４から一致性の判定結果を受信すると、ステップＳ１４５に進み、その一致性の判定結果に基づき、注目電子チケットに基づく権利が有効なものかどうかを判定する。ステップＳ１４５において、注目電子チケットに基づく権利が有効なものでないと判定された場合、即ち、有効性検証用公開鍵VPK_nによる権利証明用署名SG(r)の暗号化結果と、ステップＳ１３６で得た乱数rとの一致性が認められず、従って、チケット保持装置4_uに、注目電子チケットの有効性を表す有効性証明用秘密鍵VSK_nが存在することが認められない場合、ステップＳ１４７に進み、チケット検査制御部３１は、サービスを提供することができないことを認識し、チケット検査処理を終了する。

【０３２０】

この場合、チケット保持装置4_uのユーザは、サービス提供者からサービスの提供を受けることができない。

【０３２１】

一方、ステップＳ１４５において、注目電子チケットに基づく権利が有効なものであると判定された場合、即ち、有効性検証用公開鍵VPK_nによる権利証明用署

名SG(r)の暗号化結果と、ステップＳ１３６で得た乱数rとの一致性が認められ、従って、チケット保持装置4_uに、注目電子チケットの有効性を表す有効性証明用秘密鍵VSK_nが存在すると認められる場合、ステップＳ１４６に進み、チケット検査制御部３１は、サービスを提供することができること（サービス提供可）を認識し、チケット検査処理を終了する。

【０３２２】

この場合、チケット保持装置4_uのユーザは、サービス提供者からサービスの提供を受けることができる。

【０３２３】

一方、ステップＳ１３７において、注目電子チケットに基づく権利が、回数制限付きの権利であると判定された場合、ステップＳ１４０に進み、権利証明しようとしている電子チケットの検査を行うのかどうかが判定される。なお、チケット検査装置5_sには、例えば、権利証明または権利行使のうちのいずれについての検査を行うのかが、あらかじめ設定されており、ステップＳ１４０の判定は、その設定に基づいて行われる。

【０３２４】

ステップＳ１４０において、権利証明しようとしている電子チケットの検査を行うと判定された場合、ステップＳ１４１に進み、チケット検査制御部３１は、チケット保持装置4_uが、上述のチケットの権利行使／証明処理（図１６）を行うことによって、ステップＳ１２１で送信してくる権利証明用署名SG(r,c)と使用回数cを受信する。

【０３２５】

そして、ステップＳ１４２に進み、チケット検査制御部３１は、ステップＳ１４１で受信した権利証明用署名SG(r,c)の署名確認を行う。

【０３２６】

即ち、チケット検査制御部３１は、正当性の確認されたチケット権利条項部（図４（Ｃ））から、有効性検証用公開鍵VPK_nを抽出し、権利証明用署名SG(r,c)および使用回数cとともに、署名処理部３４に供給して、権利証明用署名SG(r,c)の署名確認を行わせる。

【０３２７】

この場合、署名処理部３４は、権利証明用署名SG(r,c)を、有効性検証用公開鍵VPK_nで暗号化処理し、その暗号化結果と、ステップＳ１３６で得た乱数rおよび使用回数cとの一致性を判定する。そして、署名処理部３４は、その一致性の判定結果を、チケット検査制御部３１に供給する。

【０３２８】

ここで、権利証明用署名SG(r,c)は、チケット保持装置4_uが、上述のチケットの権利行使／証明処理（図１６）を行うことにより、ステップＳ１２０において、有効性証明用秘密鍵VSK_nを用いて、乱数rおよび使用回数cの一方向性関数値h(r,c)を復号処理して得られるものであるから、チケット保持装置4_uおよび注目電子チケットが正当なものであれば、権利証明用署名$SG(r,c)=D(VSK_n,h(r,c))$を、有効性検証用公開鍵VPK_nで暗号化処理した暗号化結果$E(VPK_n,SG(r,c))$と、乱数rおよび使用回数cの一方向性関数値h(r,c)とは一致し、署名処理部３４では、一致性があると判定されることになる。

【０３２９】

チケット検査制御部３１は、署名処理部３４から一致性の判定結果を受信すると、ステップＳ１４５に進み、その一致性の判定結果に基づき、注目電子チケットに基づく権利が有効なものかどうかを判定する。ステップＳ１４５において、注目電子チケットに基づく権利が有効なものでないと判定された場合、即ち、有効性検証用公開鍵VPK_nによる権利証明用署名SG(r,c)の暗号化結果と、乱数rおよび使用回数cとの一致性が認められず、従って、チケット保持装置4_uに、注目電子チケットの有効性を表す有効性証明用秘密鍵VSK_nが存在することが認められない場合、ステップＳ１４７に進み、チケット検査制御部３１は、表示部３６に、電子チケットが無効である旨を表示させ、チケット検査処理を終了する。

【０３３０】

この場合、チケット保持装置4_uのユーザは、サービス提供者からサービスの提供を受けることができない。

【０３３１】

なお、注目電子チケットに基づく権利が、回数制限付き権利である場合、ステ

ップＳ１４５では、有効性検証用公開鍵VPK_nによる権利証明用署名SG(r,c)の暗号化結果と、乱数rおよび使用回数cとの一致性が認められないときの他、その一致性が認められても、使用回数cが、注目電子チケットのチケット権利条項部のチケット権利条項TIに記述されている使用回数の制限値を越えているときには、注目電子チケットに基づく権利が有効なものでないと判定される。

【０３３２】

また、ステップＳ１４５では、有効期限がある電子チケットについては、現在の日時が、注目電子チケットのチケット権利条項部のチケット権利条項TIに記述されている有効期限を越えていないかどうかも判定され、越えている場合には、注目電子チケットに基づく権利が有効なものでないと判定される。

【０３３３】

一方、ステップＳ１４５において、注目電子チケットに基づく権利が有効なものであると判定された場合、即ち、有効性検証用公開鍵VPK_nによる権利証明用署名SG(r,c)の暗号化結果と、乱数rおよび使用回数cとの一致性が認められ、従って、チケット保持装置4_uに、注目電子チケットの有効性を表す有効性証明用秘密鍵VSK_nが存在すると認められる場合であって、かつ、使用回数cが、注目電子チケットのチケット権利条項部のチケット権利条項TIに記述されている使用回数の制限値を越えていない場合、ステップＳ１４６に進み、チケット検査制御部３１は、サービスを提供することができることを認識し、チケット検査処理を終了する。

【０３３４】

この場合、チケット保持装置4_uのユーザは、サービス提供者からサービスの提供を受けることができる。

【０３３５】

一方、ステップＳ１４０において、権利証明しようとしている電子チケットの検査を行うのではないと判定された場合、即ち、権利行使しようとしている電子チケットの検査を行う場合（例えば、ユーザが、乗車券である電子チケットによって改札を通ろうとしている際に、その電子チケットの検査を行う場合）、ステップＳ１４３に進み、チケット検査制御部３１は、チケット保持装置4_uが、上

述のチケットの権利行使／証明処理（図１６）を行うことによって、ステップＳ１２３で送信してくる権利証明用署名SG(r,c,e)と使用回数cを受信する。

【０３３６】

そして、ステップＳ１４４に進み、チケット検査制御部３１は、ステップＳ１４３で受信した権利証明用署名SG(r,c,e)の署名確認を行う。

【０３３７】

即ち、チケット検査制御部３１は、正当性の確認されたチケット権利条項部（図４（Ｃ））から、有効性検証用公開鍵VPK_nを抽出し、権利証明用署名SG(r,c,e)および使用回数cとともに、署名処理部３４に供給して、権利証明用署名SG(r,c,e)の署名確認を行わせる。

【０３３８】

この場合、署名処理部３４は、権利証明用署名SG(r,c,e)を、有効性検証用公開鍵VPK_nで暗号化処理し、その暗号化結果と、ステップＳ１３６で得た乱数r、使用回数c、行使コードeとの一致性を判定する。そして、署名処理部３４は、その一致性の判定結果を、チケット検査制御部３１に供給する。

【０３３９】

ここで、権利証明用署名SG(r,c,e)は、チケット保持装置4_uが、上述のチケットの権利行使／証明処理（図１６）を行うことにより、ステップＳ１２２において、有効性証明用秘密鍵VSK_nを用いて、乱数r、使用回数c、および行使コードeの一方向性関数値h(r,c,e)を復号処理して得られるものであるから、チケット保持装置4_uおよび注目電子チケットが正当なものであれば、権利証明用署名SG(r,c,e)=$D(VSK_n,h(r,c,e))$を、有効性検証用公開鍵VPK_nで暗号化処理した暗号化結果$E(VPK_n,SG(r,c,e))$と、乱数r、使用回数c、および行使コードeの一方向性関数値h(r,c,e)とは一致し、署名処理部３４では、一致性があると判定されることになる。

【０３４０】

チケット検査制御部３１は、署名処理部３４から一致性の判定結果を受信すると、ステップＳ１４５に進み、その一致性の判定結果に基づき、注目電子チケットに基づく権利が有効なものかどうかを判定する。ステップＳ１４５において、

注目電子チケットに基づく権利が有効なものでないと判定された場合、即ち、有効性検証用公開鍵VPK_nによる権利証明用署名SG(r,c,r)の暗号化結果と、乱数r、使用回数c、および行使コードeとの一致性が認められず、従って、チケット保持装置4_uに、注目電子チケットの有効性を表す有効性証明用秘密鍵VSK_nが存在することが認められない場合、あるいは、チケット保持装置4_uからの権利証明用署名SGに、正当な行使コードeが存在することが認められない場合、ステップＳ１４７に進み、チケット検査制御部３１は、サービスを提供することができないことを認識し、チケット検査処理を終了する。

【０３４１】

この場合、チケット保持装置4_uのユーザは、サービス提供者からサービスの提供を受けることができない。

【０３４２】

なお、権利行使しようとしている電子チケットの検査の場合においても、権利証明しようとしている電子チケットの検査における場合と同様に、ステップＳ１４５では、使用回数cが、注目電子チケットのチケット権利条項部のチケット権利条項TIに記述されている使用回数の制限値を越えているかどうかや、現在の日時が、注目電子チケットのチケット権利条項部のチケット権利条項TIに記述されている有効期限を越えていないかどうか等も判定される。

【０３４３】

一方、ステップＳ１４５において、注目電子チケットに基づく権利が有効なものであると判定された場合、即ち、有効性検証用公開鍵VPK_nによる権利証明用署名SG(r,c,e)の暗号化結果と、乱数r、使用回数c、および行使コードeとの一致性が認められ、従って、チケット保持装置4_uに、注目電子チケットの有効性を表す有効性証明用秘密鍵VSK_nが存在すると認められる場合であって、かつ、使用回数cが、注目電子チケットのチケット権利条項部のチケット権利条項TIに記述されている使用回数の制限値を越えておらず、さらに、権利証明用署名SG(r,c,e)に、正当な行使コードeが含まれている場合、ステップＳ１４６に進み、チケット検査制御部３１は、サービスを提供することができることを認識し、チケット検査処理を終了する。

【０３４４】

この場合、チケット保持装置４$_u$のユーザは、サービス提供者からサービスの提供を受けることができる。

【０３４５】

次に、上述した一連の処理は、ハードウェアにより行うこともできるし、ソフトウェアにより行うこともできる。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータ等にインストールされる。

【０３４６】

そこで、図１９は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【０３４７】

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク１０５やＲＯＭ１０３に予め記録しておくことができる。

【０３４８】

あるいはまた、プログラムは、フロッピーディスク、CD-ROM(Compact Disc Read Only Memory)，MO(Magneto optical)ディスク，DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体１１１に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体１１１は、いわゆるパッケージソフトウエアとして提供することができる。

【０３４９】

なお、プログラムは、上述したようなリムーバブル記録媒体１１１からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部１０８で受信し、内蔵するハードディスク１０５にインストールすることができる。

【０３５０】

コンピュータは、CPU(Central Processing Unit)１０２を内蔵している。CPU１０２には、バス１０１を介して、入出力インタフェース１１０が接続されており、CPU１０２は、入出力インタフェース１１０を介して、ユーザによって、キーボードや、マウス、マイク等で構成される入力部１０７が操作等されることにより指令が入力されると、それにしたがって、ROM(Read Only Memory)１０３に格納されているプログラムを実行する。あるいは、また、CPU１０２は、ハードディスク１０５に格納されているプログラム、衛星若しくはネットワークから転送され、通信部１０８で受信されてハードディスク１０５にインストールされたプログラム、またはドライブ１０９に装着されたリムーバブル記録媒体１１１から読み出されてハードディスク１０５にインストールされたプログラムを、RAM(Random Access Memory)１０４にロードして実行する。これにより、CPU１０２は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU１０２は、その処理結果を、必要に応じて、例えば、入出力インタフェース１１０を介して、LCD(Liquid CryStal Display)やスピーカ等で構成される出力部１０６から出力、あるいは、通信部１０８から送信、さらには、ハードディスク１０５に記録等させる。

【０３５１】

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【０３５２】

また、プログラムは、１のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【０３５３】

以上のように、乗車券や、入場券、予約券、会員権許可書、サービス券などの

従来のチケットを電子情報化し、ネットワークなどの電気的な通信経路を経由してやり取りすることができる電子チケットを、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な有効性証明用秘密鍵VSK_nを含み、電子チケットの有効性を証明するためのチケット有効性部と、有効性証明用秘密鍵VSK_nが存在することを検証するのに用いられる有効性検証用公開鍵VPK_nを含み、有効性証明用秘密鍵VSK_nによって、その有効性が証明されるチケット権利条項部とによって構成するようにしたので、従来のチケットが有する機能を備える電子チケットの流通を可能にすることができる。

【０３５４】

即ち、電子チケットの複製によって、その電子チケットに基づく権利を不正に利用されることを防ぐ機能である「権利複製防止」、匿名の第三者に対する場合も含めて、電子チケットに基づく権利を証明する機能である「権利証明」、電子チケットを使用するユーザの匿名性を保証する機能である「匿名性」、電子チケットに基づく権利を他人に譲ることができる機能である「譲渡性」、および電子チケットに基づく権利の確認を、その電子チケットだけで行うことのでできる機能である「完結性」を備える、利便性の高い電子チケットの流通を可能にすることができる。

【０３５５】

また、電子チケットのチケット有効性部には、有効性証明用秘密鍵VSK_nの他、使用回数等の付加情報を含めることができるので、使用回数の制限が可能な、利便性の高い電子チケットを実現することができる。さらに、この場合、使用回数の改竄を防止することができる。

【０３５６】

なお、本実施の形態においては、本発明を電子チケットシステムに適用した場合について説明したが、本発明は、その他、例えば、コンピュータに実行させるプログラムにも適用することが可能である。即ち、チケット権利条項部のチケット権利条項TIに替えてプログラムを配置し、チケット保持装置４_uを、プログラムの保持装置とするとともに、プログラムの実行に際して、コンピュータにおけるオペレーティングシステム、アプリケーションプログラム、あるいは保持装置

に保持されたプログラムの一部に、チケット検査装置５$_s$の機能を持たせて、プログラムの使用等に関する権利の検査を行うようにすることで、プログラムの不正使用を防止する等の、プログラムに関する著作権等の権利を保護することが可能となる。

【０３５７】

また、本実施の形態では、公開鍵暗号化方式、共通鍵暗号化方式、および電子署名を利用するようにしたが、これらの公開鍵暗号化方式、共通鍵暗号化方式、および電子署名として採用する具体的なアルゴリズムは、特に限定されるものではない。

【０３５８】

【発明の効果】

本発明の情報記録媒体によれば、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データと、秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報とが記録されている。従って、例えば、利便性の高い電子チケットを実現することが可能となる。

【０３５９】

本発明の第１の情報処理装置および情報処理方法、並びにプログラム記録媒体によれば、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データが生成されるとともに、秘密情報が存在することを検証するのに用いられる検証用パラメータが生成される。そして、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が生成され、有効性データと被証明情報とからなる情報セットが外部に出力される。従って、例えば、利便性の高い電子チケットを発行することが可能となる。

【０３６０】

本発明の第２の情報処理装置および情報処理方法、並びにプログラム記録媒体によれば、それ自体を外部に示すことなく、それが存在することを証明すること

ができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が、その被証明情報を検査する検査装置に送信される。さらに、秘密情報の存在を証明する証明データが生成され、検査装置に送信される。従って、例えば、電子チケットを、従来の紙等によるチケットと同様に扱うことが可能となる。

【０３６１】

本発明の第３の情報処理装置および情報処理方法、並びにプログラム記録媒体によれば、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含む、情報の有効性を証明するための有効性データにおける秘密情報が存在することを検証するのに用いられる検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が受信されるとともに、秘密情報の存在を証明する証明データが受信される。そして、証明データと、被証明情報に含まれる検証用パラメータとを用いて、他の装置における秘密情報の存否が判定される。従って、例えば、電子チケットを、従来の紙等によるチケットと同様に扱うことが可能となる。

【０３６２】

本発明の情報処理システムによれば、第１の情報処理装置において、それ自体を外部に示すことなく、それが存在することを証明することができるアルゴリズムが適用可能な秘密情報を含み、情報の有効性を証明するための有効性データが生成されるとともに、秘密情報が存在することを検証するのに用いられる検証用パラメータが生成される。さらに、検証用パラメータを含み、有効性データによって、その有効性が証明される被証明情報が生成され、有効性データと被証明情報とからなる情報セットが発行される。第２の情報処理装置では、被証明情報が、その被証明情報を検査する第３の情報処理装置に送信されるとともに、秘密情報の存在を証明する証明データが生成され、第３の情報処理装置に送信される。第３の情報処理装置では、第２の情報処理装置からの被証明情報が受信されるとともに、第２の情報処理装置からの秘密情報の存在を証明する証明データが受信され、証明データと、被証明情報に含まれる検証用パラメータとを用いて、第２

の情報処理装置における秘密情報の存否が判定される。従って、例えば、利便性の高い電子チケットを流通させることが可能となる。

【図面の簡単な説明】

【図１】

本発明を適用した電子チケットシステムの一実施の形態の構成例を示す図である。

【図２】

チケット管理センタ１の役割を説明する図である。

【図３】

チケット管理センタ１の役割を説明する図である。

【図４】

電子チケットのデータフォーマットを示す図である。

【図５】

チケット発行装置３_{t}の構成例を示すブロック図である。

【図６】

チケット発行処理を説明するフローチャートである。

【図７】

チケット保持装置４_{u}の構成例を示すブロック図である。

【図８】

ストレージ部２８の記憶内容を示す図である。

【図９】

チケット譲受処理を説明するフローチャートである。

【図１０】

譲受側の認証処理を説明するフローチャートである。

【図１１】

チケット権利条項部の確認処理を説明するフローチャートである。

【図１２】

チケット追加処理を説明するフローチャートである。

【図１３】

チケット譲渡処理を説明するフローチャートである。

【図１４】

譲渡側の認証処理を説明するフローチャートである。

【図１５】

チケット削除処理を説明するフローチャートである。

【図１６】

チケットの権利行使／証明処理を説明するフローチャートである。

【図１７】

チケット検査装置5_Sの構成例を示すブロック図である。

【図１８】

チケット検査処理を説明するフローチャートである。

【図１９】

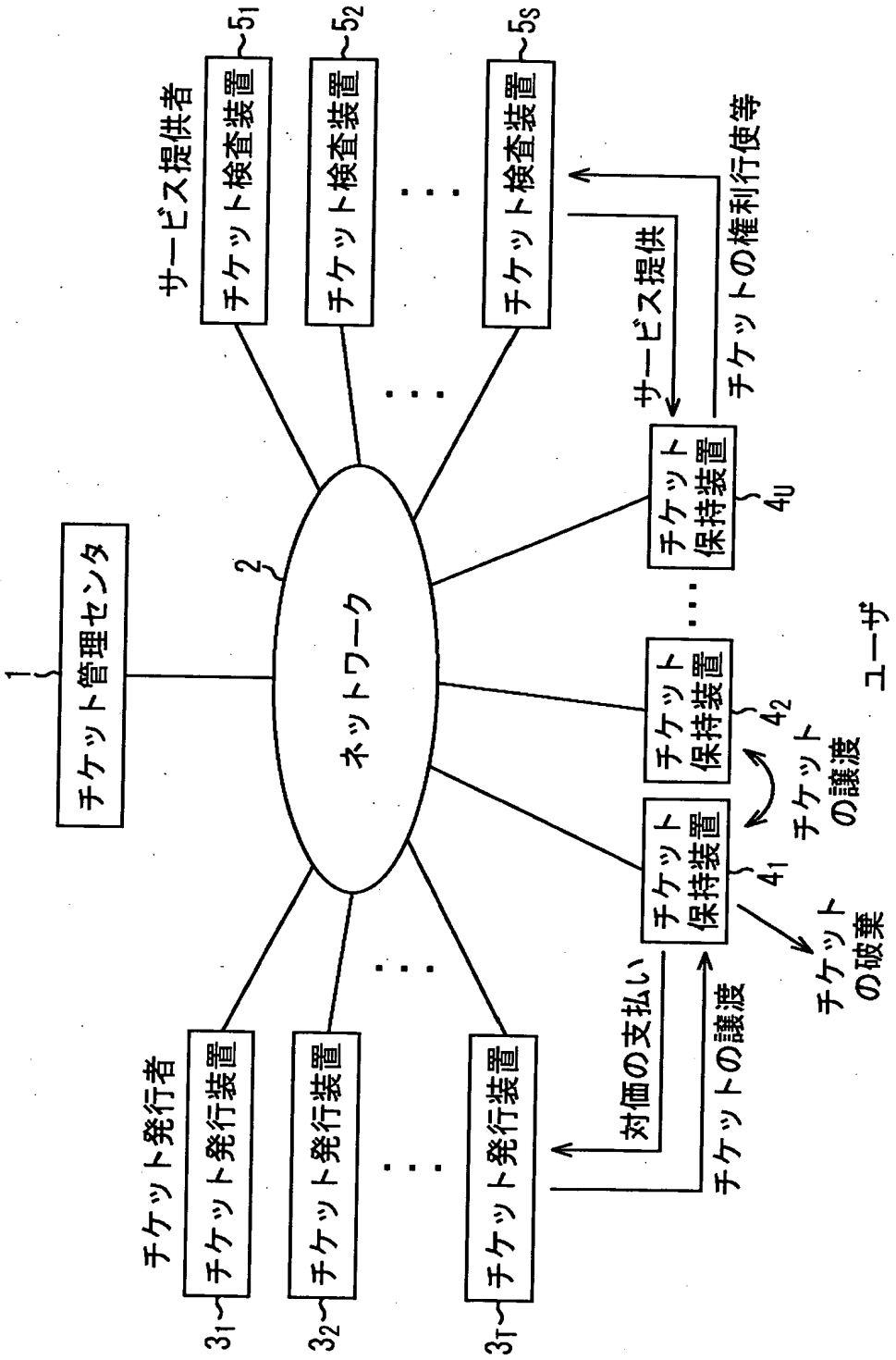
本発明を適用したコンピュータの一実施の形態の構成例を示すブロック図である。

【符号の説明】

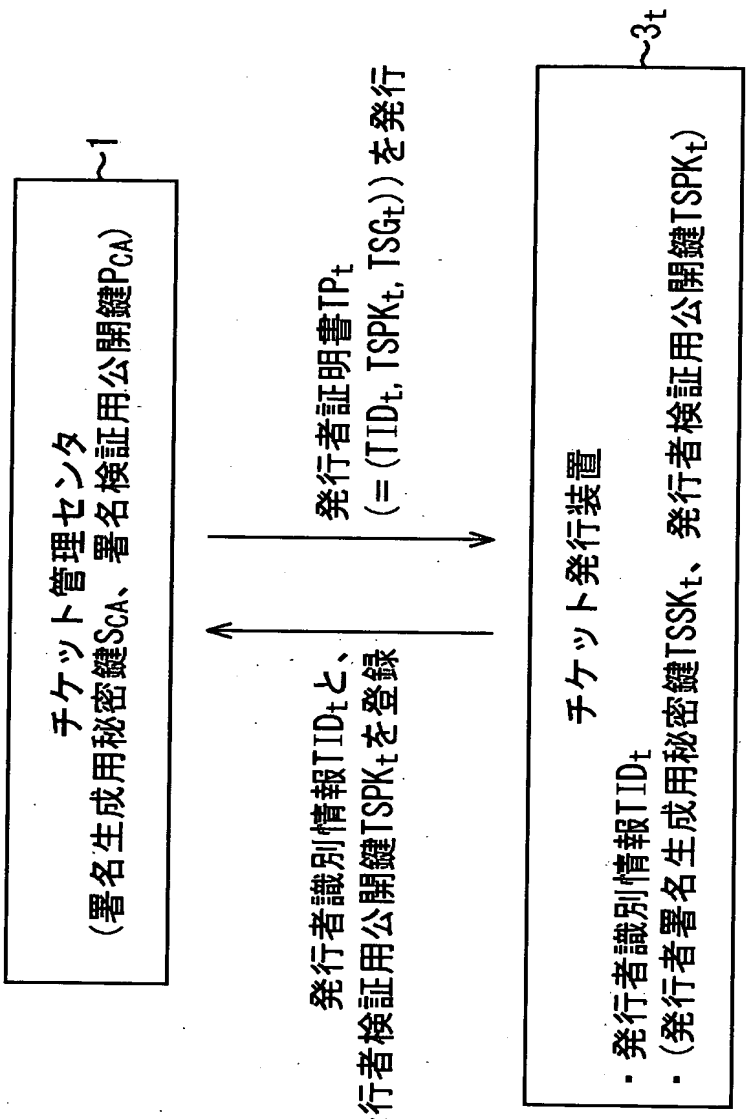
１　チケット管理センタ，　２　ネットワーク，　3_1乃至3_T　チケット発行装置，　4_1乃至4_U　チケット保持装置，　5_1乃至5_S　チケット検査装置，　１１　チケット条項取得部，　１２　発行者証明書取得部，　１３　発行者署名生成用秘密鍵取得部，　１４　乱数発生部，　１５　有効性鍵生成部，　１６　条項検証用署名生成部，　１７　チケット生成部，　１８　チケット保持発行制御部，　２１　チケット授受制御部，　２２　装置証明書記憶部，　２３　乱数発生部，　２４　署名処理部，　２５　署名検証用公開鍵記憶部，　２６　公開鍵暗号処理部，　２７　管理部，　２７Ａ　親共通鍵記憶部，　２８　ストレージ部，　２９　共通鍵暗号処理部，　３１　チケット検査制御部，　３２　乱数発生部，　３３　検査内容記憶部，　３４　署名処理部，　３５　署名検証用公開鍵記憶部，　３６　表示部，　１０１　バス，　１０２　CPU，　１０３　ROM，　１０４　RAM，　１０５　ハードディスク，　１０６　出力部，　１０７　入力部，　１０８　通信部，　１０９　ドライブ，　１１０　入出力インタフェース，　１１１　リムーバブル記録媒体

【書類名】図面

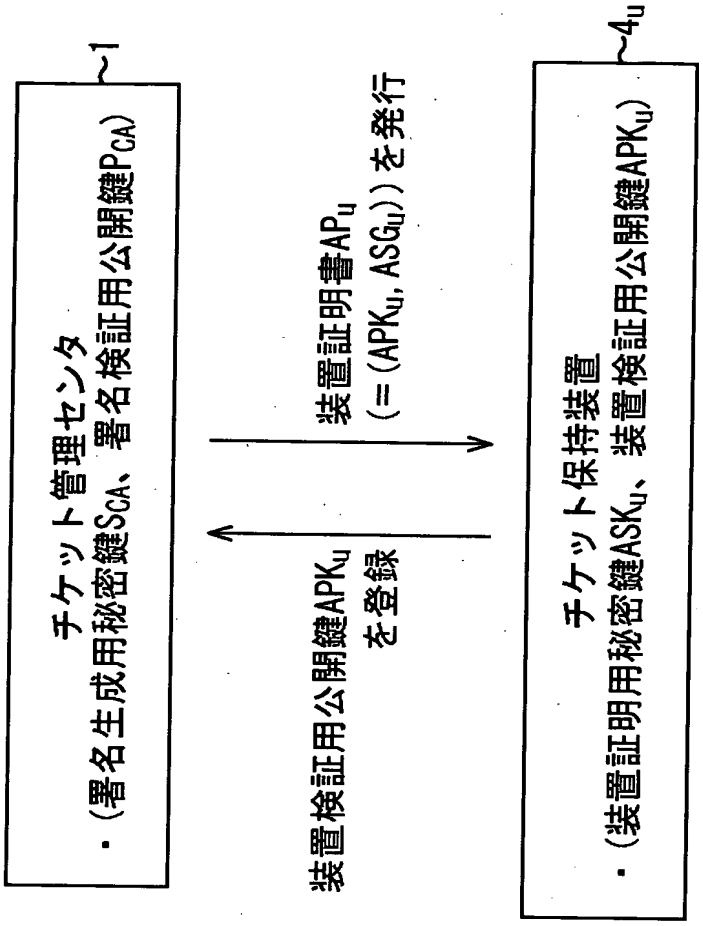
【図１】


チケット管理センタ
1
ネットワーク
2
サービス提供者
チケット検査装置
5_1
チケット検査装置
5_2
チケット検査装置
5_S
サービス提供
チケットの権利行使等
チケット保持装置
4_U
チケット保持装置
4_2
チケット保持装置
4_1
ユーザ
チケットの譲渡
チケットの破棄
対価の支払い
チケットの譲渡
チケット発行者
チケット発行装置
3_1
チケット発行装置
3_2
チケット発行装置
3_T
電子チケットシステム

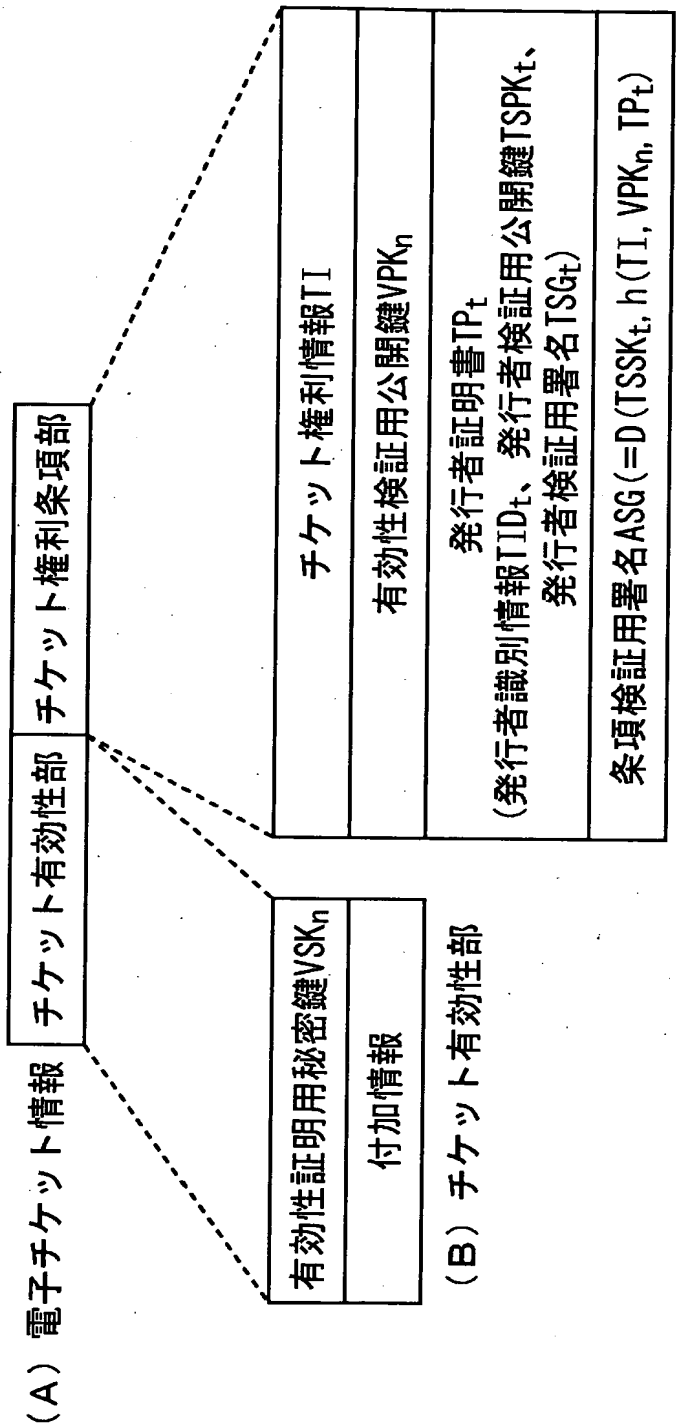
【図２】


チケット管理センタ
(署名生成用秘密鍵S_{CA}、署名検証用公開鍵P_{CA})
~1
発行者識別情報TID_tと、
発行者検証用公開鍵$TSPK_t$を登録
発行者証明書TP_t
(=(TID_t, $TSPK_t$, TSG_t))を発行
チケット発行装置
~3t
・発行者識別情報TID_t
・(発行者署名生成用秘密鍵$TSSK_t$、発行者検証用公開鍵$TSPK_t$)

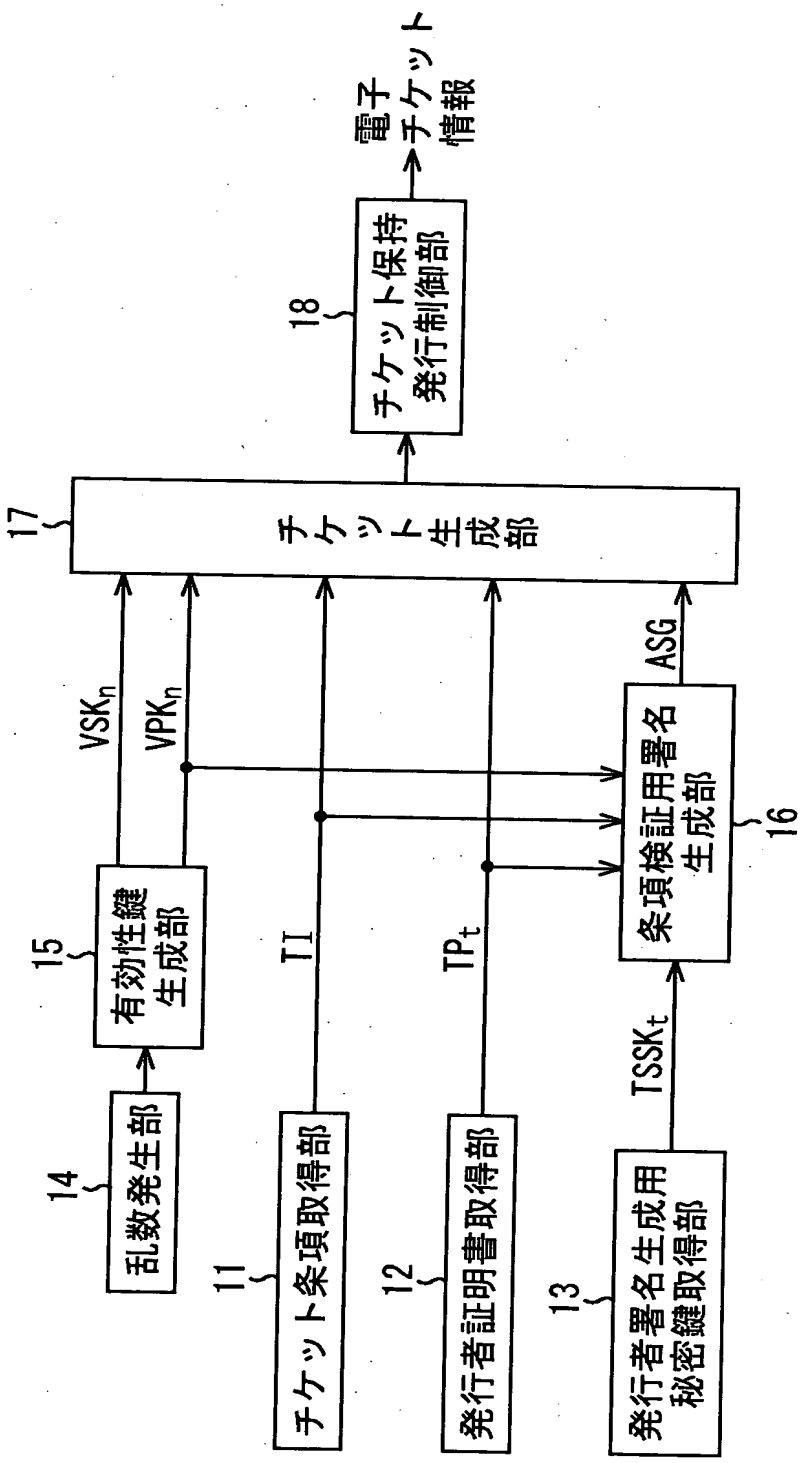
【図３】


チケット管理センタ
・(署名生成用秘密鍵S_{CA}、署名検証用公開鍵P_{CA})
~1
装置検証用公開鍵APK_U
を登録
装置証明書AP_U
(=(APK_U, ASG_U))を発行
チケット保持装置
・(装置証明用秘密鍵ASK_U、装置検証用公開鍵APK_U)
~4_U

【図４】

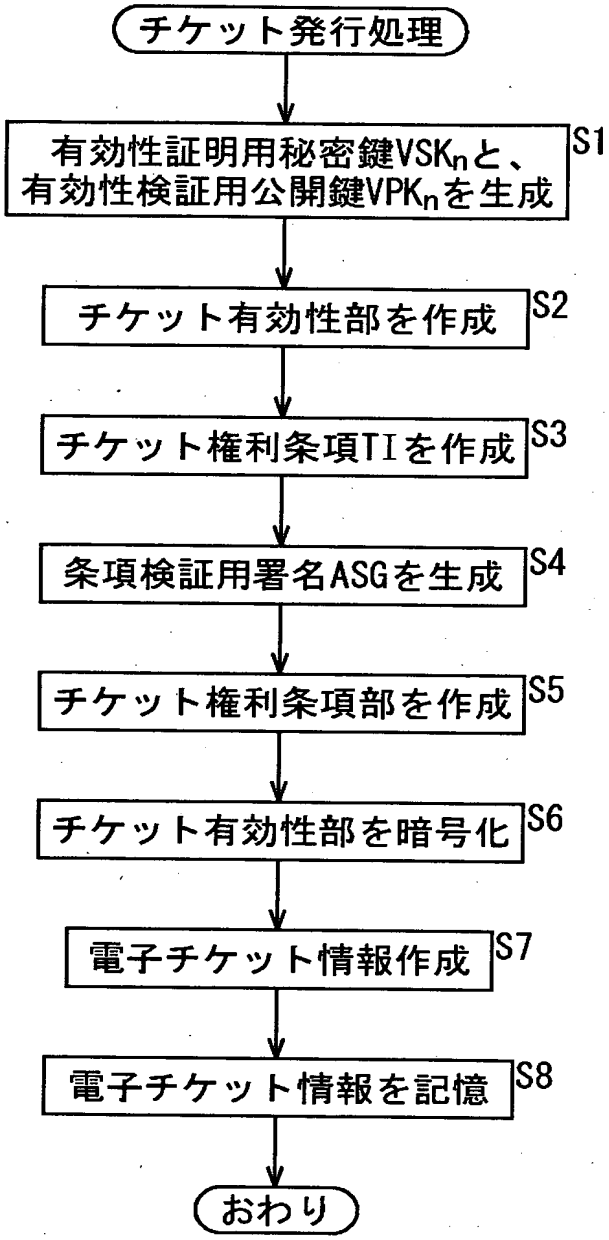

（A）電子チケット情報
チケット有効性部
チケット権利条項部
有効性証明用秘密鍵VSKn
付加情報
チケット権利情報TI
有効性検証用公開鍵VPKn
発行者証明書TPt
（発行者識別情報TIDt、発行者検証用公開鍵TSPKt、
発行者検証用署名TSGt）
条項検証用署名ASG(=D(TSSKt, h(TI, VPKn, TPt)
（B）チケット有効性部
（C）チケット権利条項部

【図５】

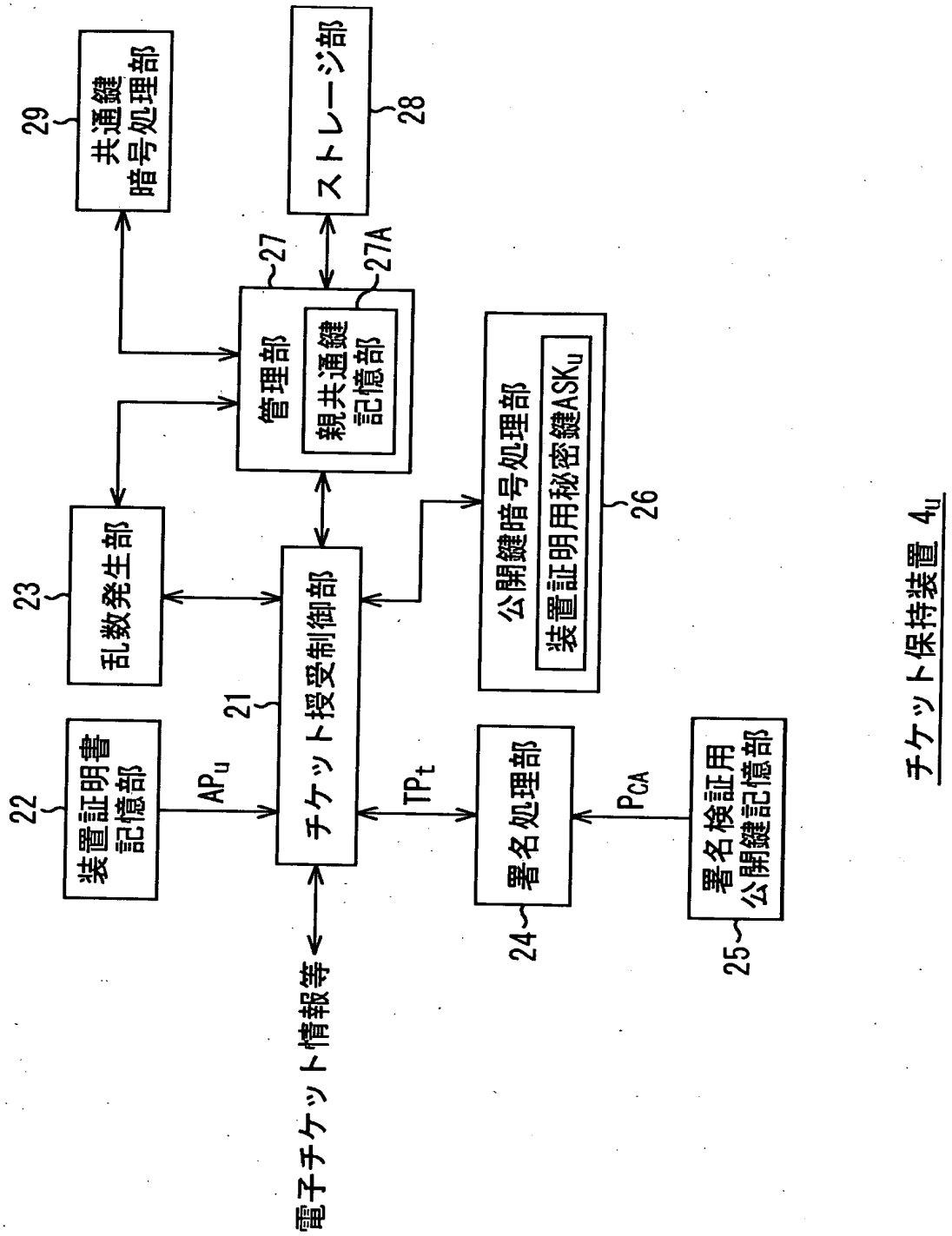


チケット発行装置 3$_t$

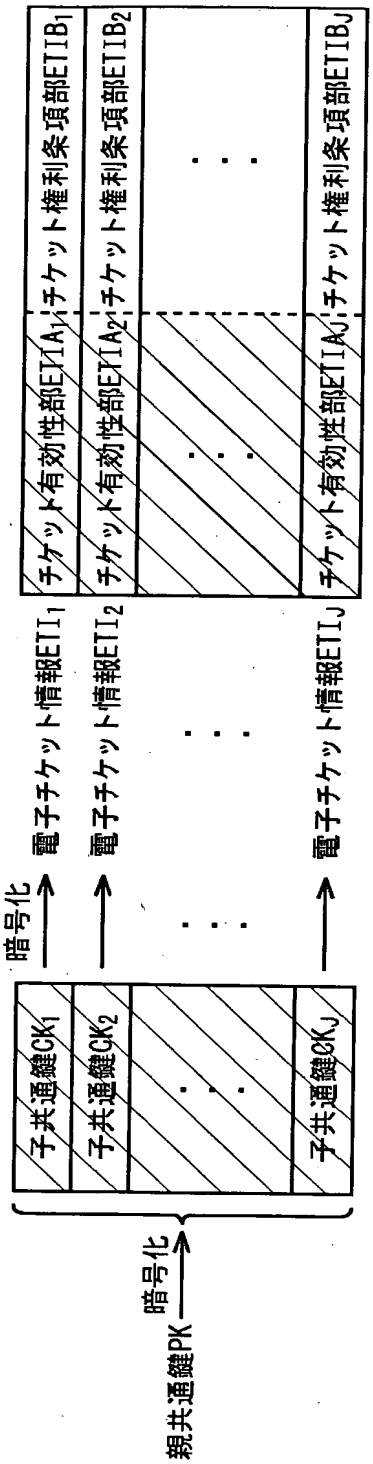
【図６】


チケット発行処理
有効性証明用秘密鍵VSKnと、
有効性検証用公開鍵VPKnを生成
S1
チケット有効性部を作成
S2
チケット権利条項TIを作成
S3
条項検証用署名ASGを生成
S4
チケット権利条項部を作成
S5
チケット有効性部を暗号化
S6
電子チケット情報作成
S7
電子チケット情報を記憶
S8
おわり

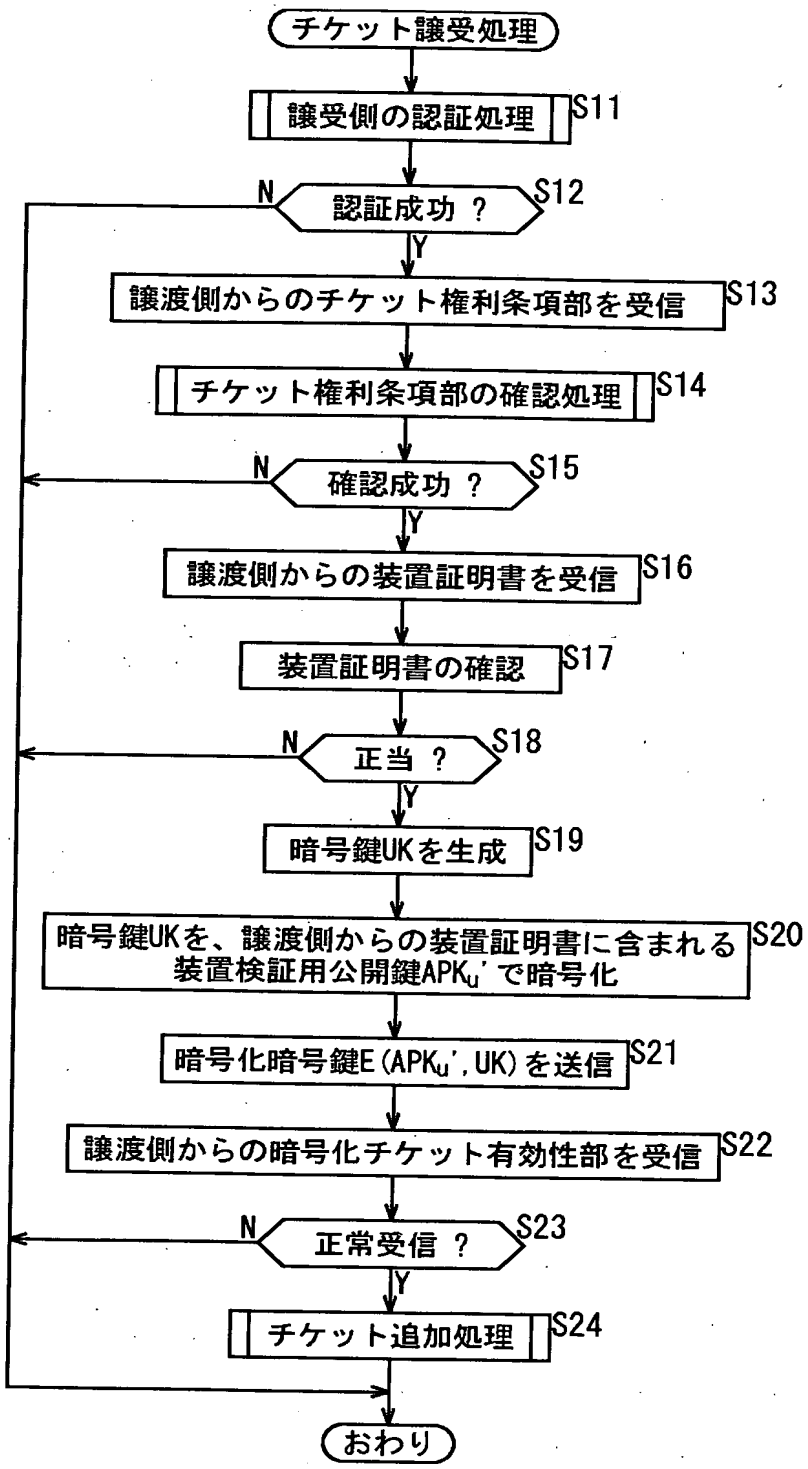
【図７】


チケット保持装置 4_U
電子チケット情報等
チケット授受制御部
21
装置証明書記憶部
22
AP_U
乱数発生部
23
署名処理部
24
TP_t
署名検証用公開鍵記憶部
25
P_{CA}
公開鍵暗号処理部
装置証明用秘密鍵ASK_U
26
管理部
親共通鍵記憶部
27
27A
ストレージ部
28
共通鍵暗号処理部
29

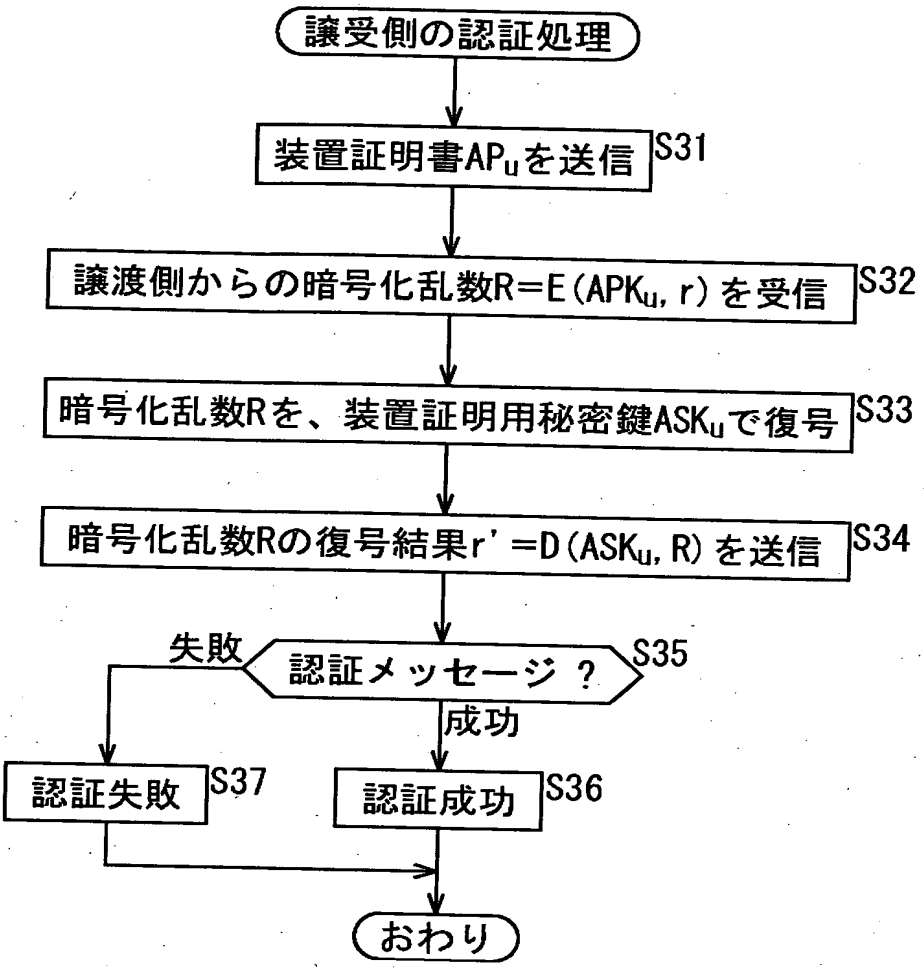
【図８】


親共通鍵PK
暗号化
子共通鍵CK1
子共通鍵CK2
子共通鍵CKJ
暗号化
電子チケット情報ETI1
電子チケット情報ETI2
電子チケット情報ETIJ
チケット有効性部ETIA1
チケット権利条項部ETIB1
チケット有効性部ETIA2
チケット権利条項部ETIB2
チケット有効性部ETIAJ
チケット権利条項部ETIBJ
（B）管理情報
（A）電子チケット情報
ストレージ部の記憶内容

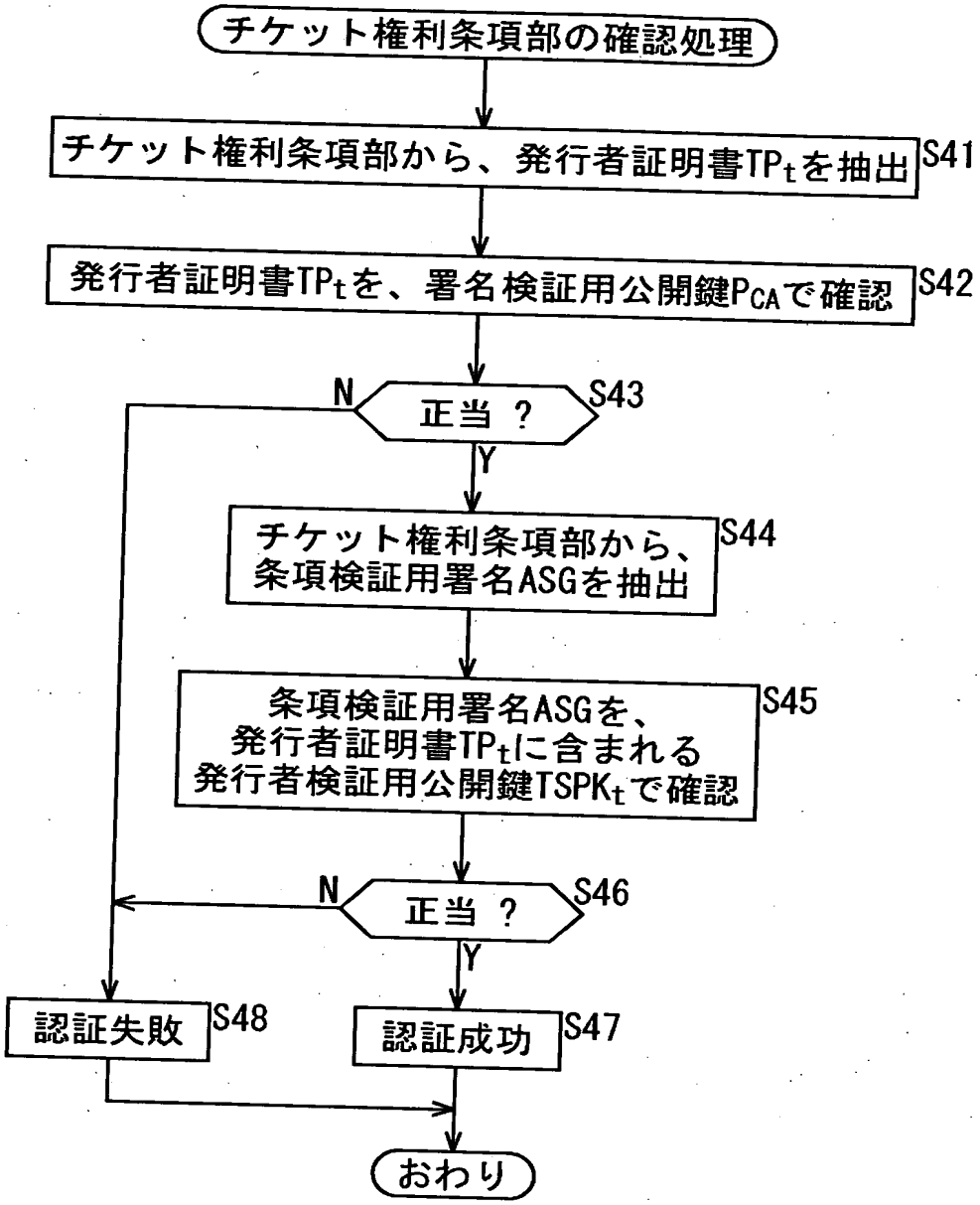
【図９】


チケット譲受処理
譲受側の認証処理
S11
N
認証成功 ？
S12
Y
譲渡側からのチケット権利条項部を受信
S13
チケット権利条項部の確認処理
S14
N
確認成功 ？
S15
Y
譲渡側からの装置証明書を受信
S16
装置証明書の確認
S17
N
正当 ？
S18
Y
暗号鍵UKを生成
S19
暗号鍵UKを、譲渡側からの装置証明書に含まれる
装置検証用公開鍵APKu'で暗号化
S20
暗号化暗号鍵E(APKu', UK)を送信
S21
譲渡側からの暗号化チケット有効性部を受信
S22
N
正常受信 ？
S23
Y
チケット追加処理
S24
おわり

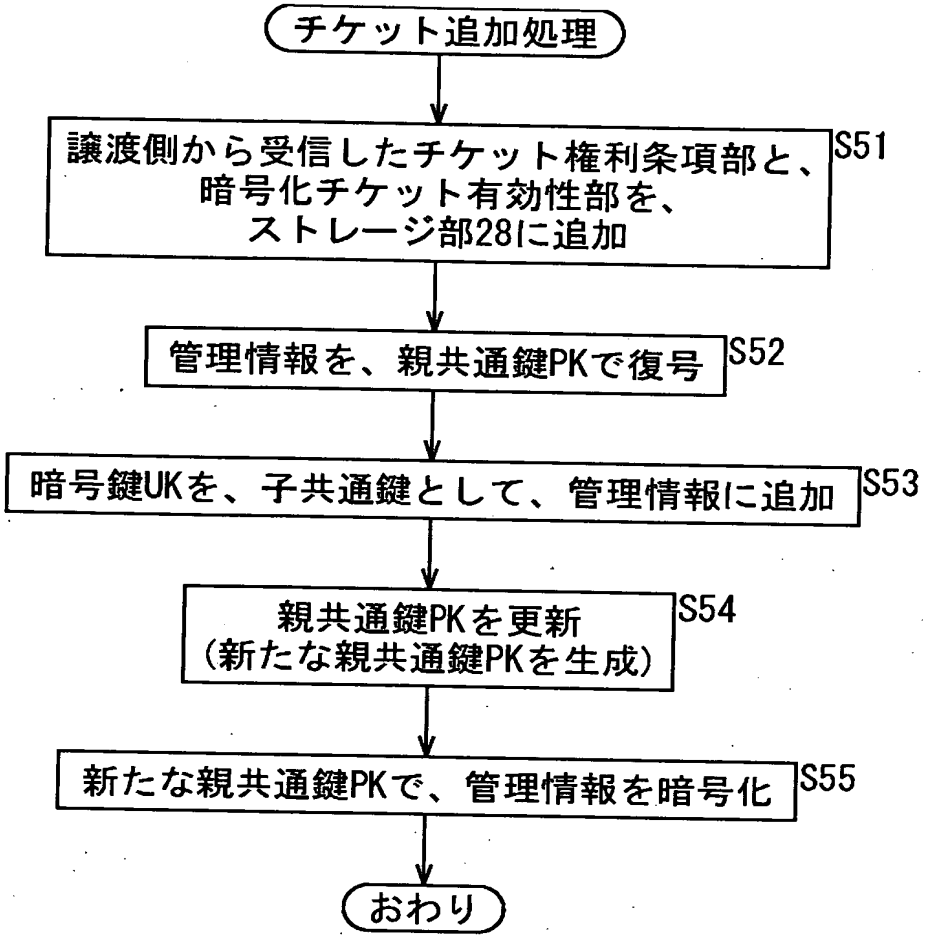
【図１０】


譲受側の認証処理
装置証明書APuを送信
S31
譲渡側からの暗号化乱数R=E(APKu, r)を受信
S32
暗号化乱数Rを、装置証明用秘密鍵ASKuで復号
S33
暗号化乱数Rの復号結果r'=D(ASKu, R)を送信
S34
失敗
認証メッセージ？
S35
成功
認証失敗
S37
認証成功
S36
おわり

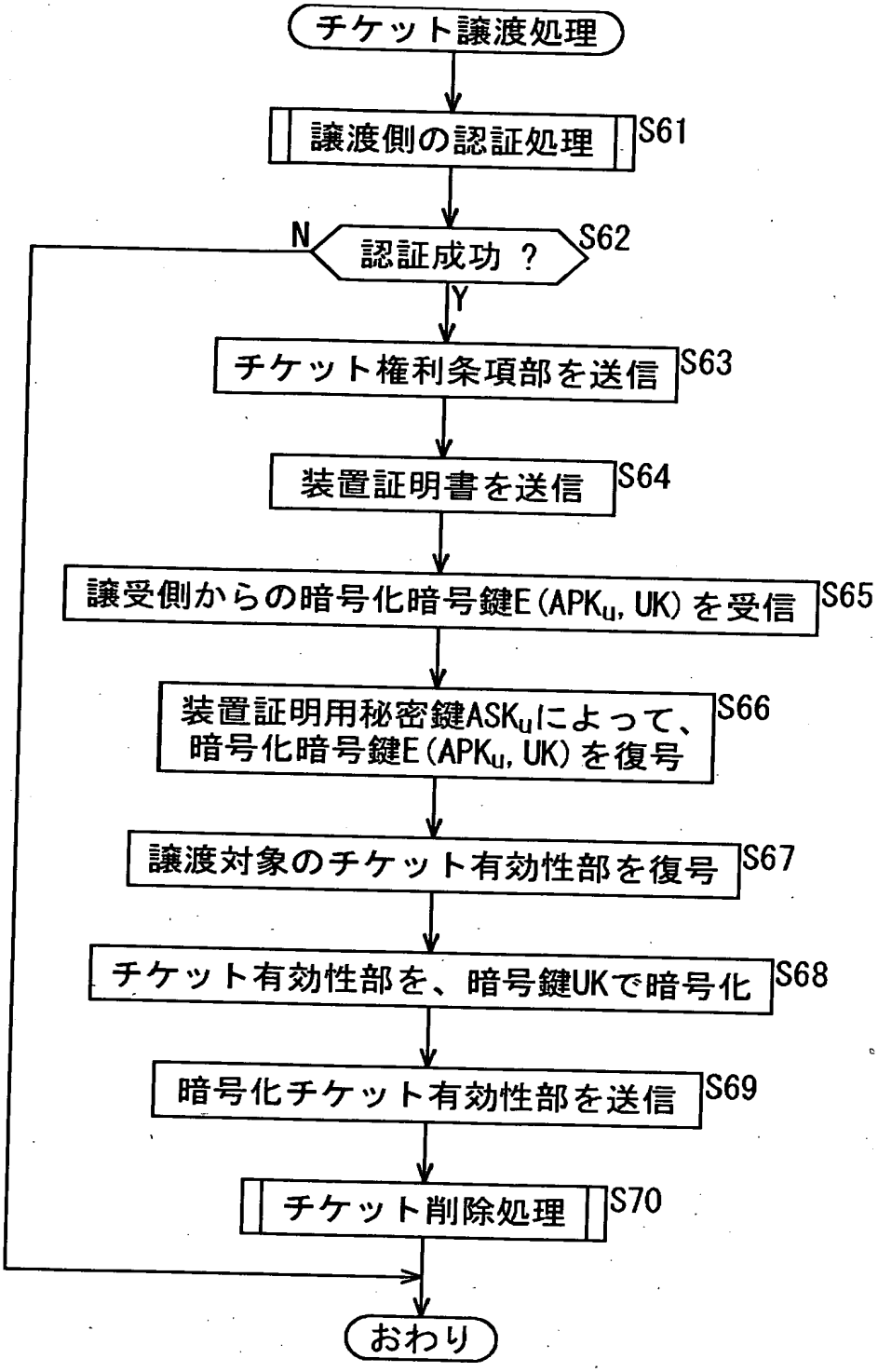
【図１１】


チケット権利条項部の確認処理
チケット権利条項部から、発行者証明書TPtを抽出
S41
発行者証明書TPtを、署名検証用公開鍵PCAで確認
S42
N
正当 ？
S43
Y
チケット権利条項部から、
条項検証用署名ASGを抽出
S44
条項検証用署名ASGを、
発行者証明書TPtに含まれる
発行者検証用公開鍵TSPKtで確認
S45
N
正当 ？
S46
Y
認証失敗
S48
認証成功
S47
おわり

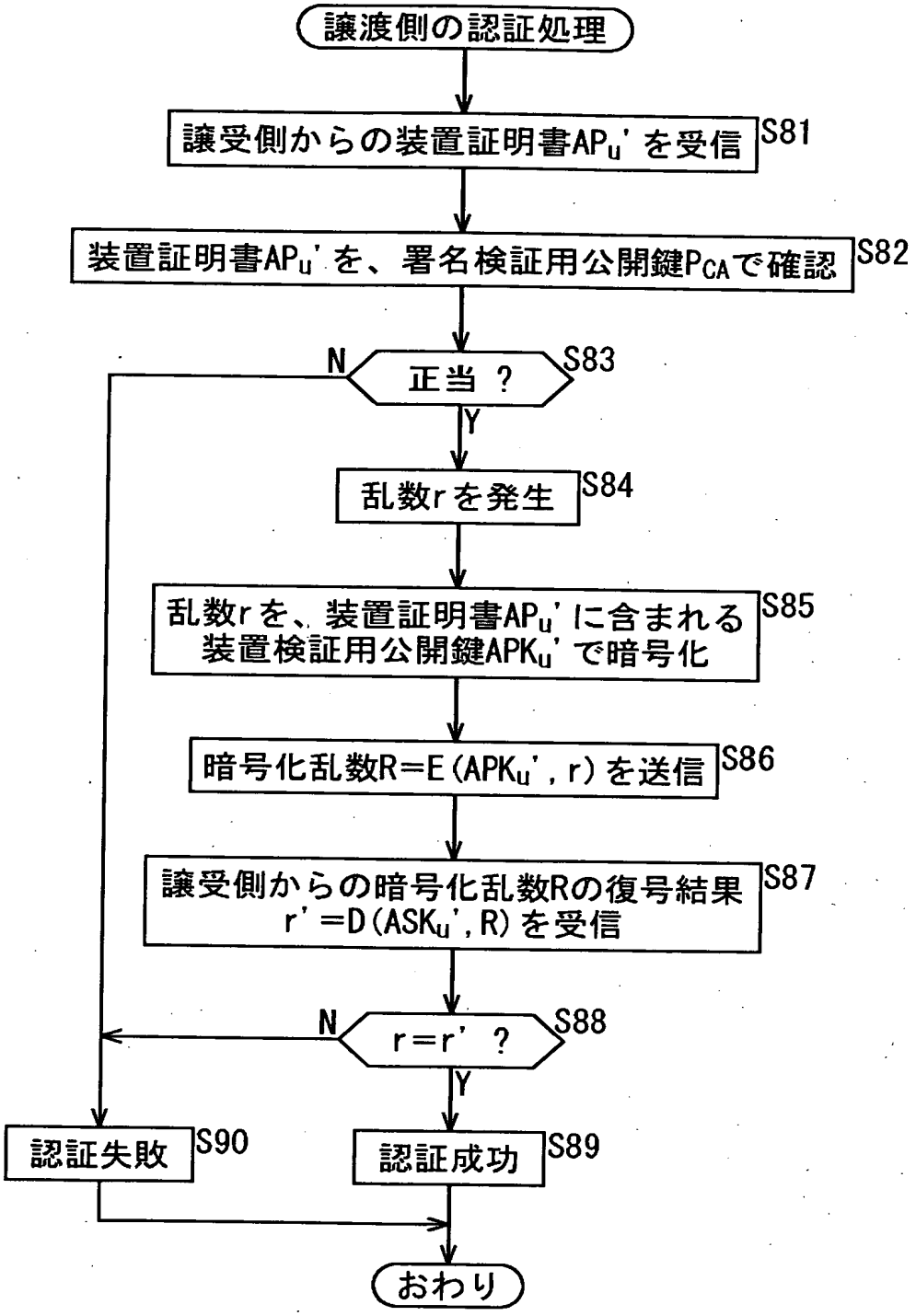
【図１２】


チケット追加処理
譲渡側から受信したチケット権利条項部と、暗号化チケット有効性部を、ストレージ部28に追加
S51
管理情報を、親共通鍵PKで復号
S52
暗号鍵UKを、子共通鍵として、管理情報に追加
S53
親共通鍵PKを更新（新たな親共通鍵PKを生成）
S54
新たな親共通鍵PKで、管理情報を暗号化
S55
おわり

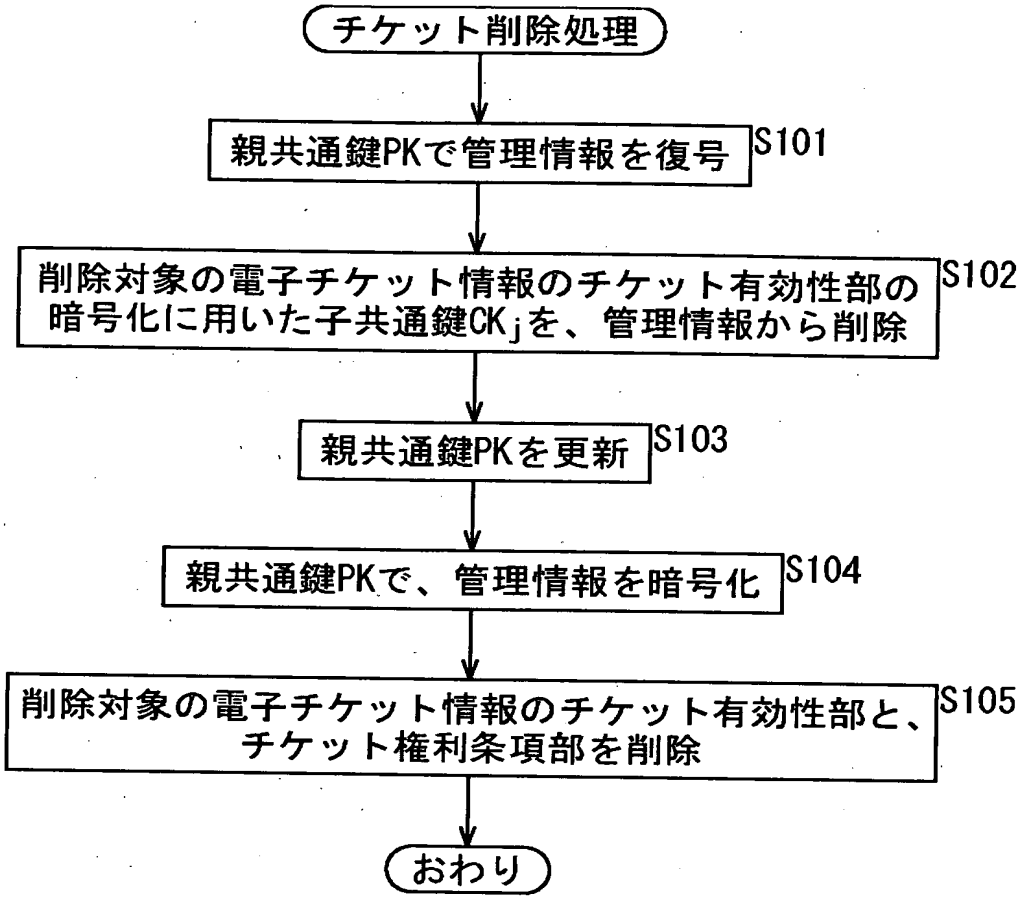
【図１３】


チケット譲渡処理
譲渡側の認証処理
S61
N
認証成功 ？
S62
Y
チケット権利条項部を送信
S63
装置証明書を送信
S64
譲受側からの暗号化暗号鍵E(APKu, UK)を受信
S65
装置証明用秘密鍵ASKuによって、
暗号化暗号鍵E(APKu, UK)を復号
S66
譲渡対象のチケット有効性部を復号
S67
チケット有効性部を、暗号鍵UKで暗号化
S68
暗号化チケット有効性部を送信
S69
チケット削除処理
S70
おわり

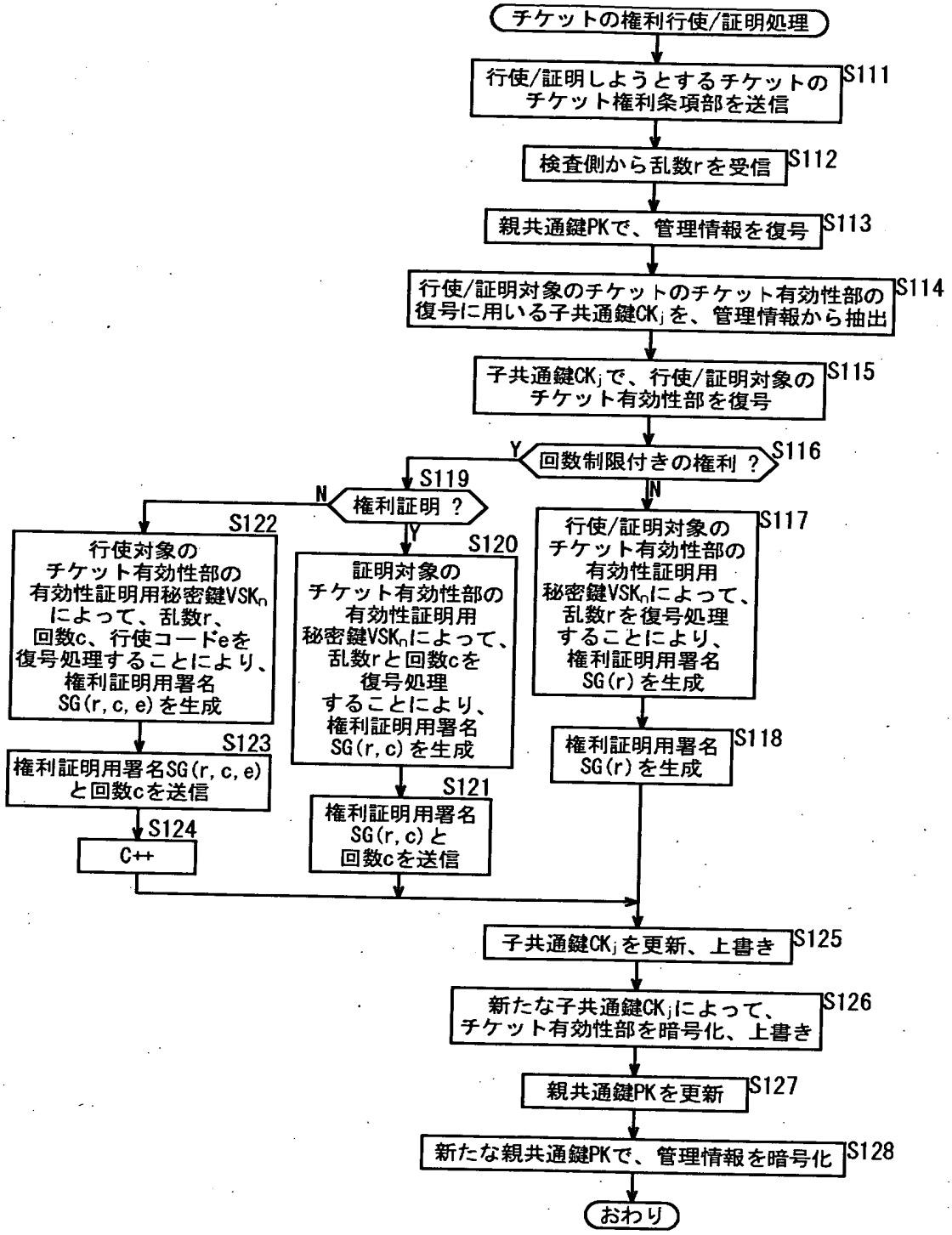
【図１４】


譲渡側の認証処理
譲受側からの装置証明書APu'を受信
S81
装置証明書APu'を、署名検証用公開鍵PCAで確認
S82
N
正当 ?
S83
Y
乱数rを発生
S84
乱数rを、装置証明書APu'に含まれる
装置検証用公開鍵APKu'で暗号化
S85
暗号化乱数R=E(APKu', r)を送信
S86
譲受側からの暗号化乱数Rの復号結果
r'=D(ASKu', R)を受信
S87
N
r=r' ?
S88
Y
認証失敗
S90
認証成功
S89
おわり

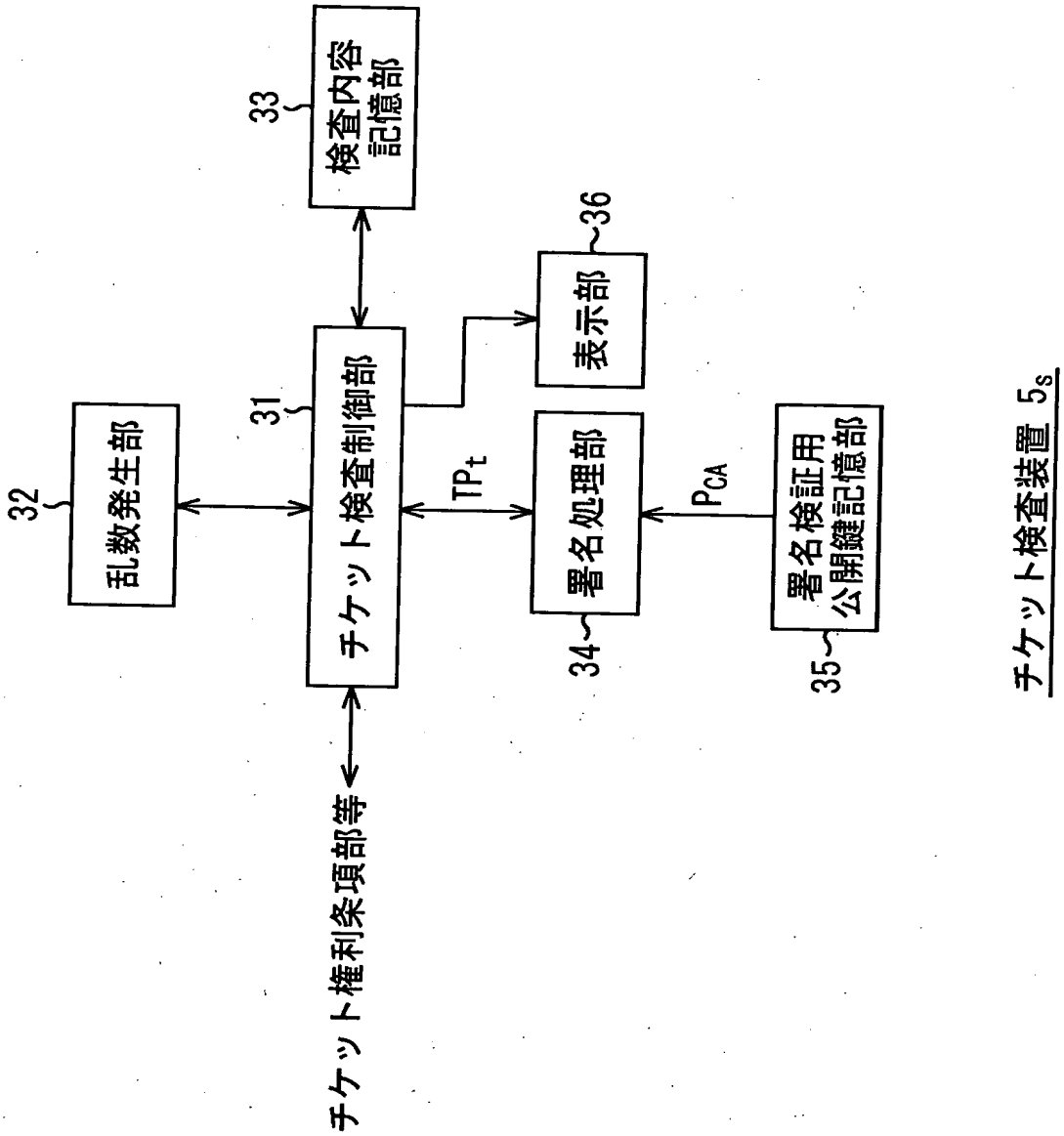
【図１５】


チケット削除処理
親共通鍵PKで管理情報を復号
S101
削除対象の電子チケット情報のチケット有効性部の暗号化に用いた子共通鍵CKjを、管理情報から削除
S102
親共通鍵PKを更新
S103
親共通鍵PKで、管理情報を暗号化
S104
削除対象の電子チケット情報のチケット有効性部と、チケット権利条項部を削除
S105
おわり

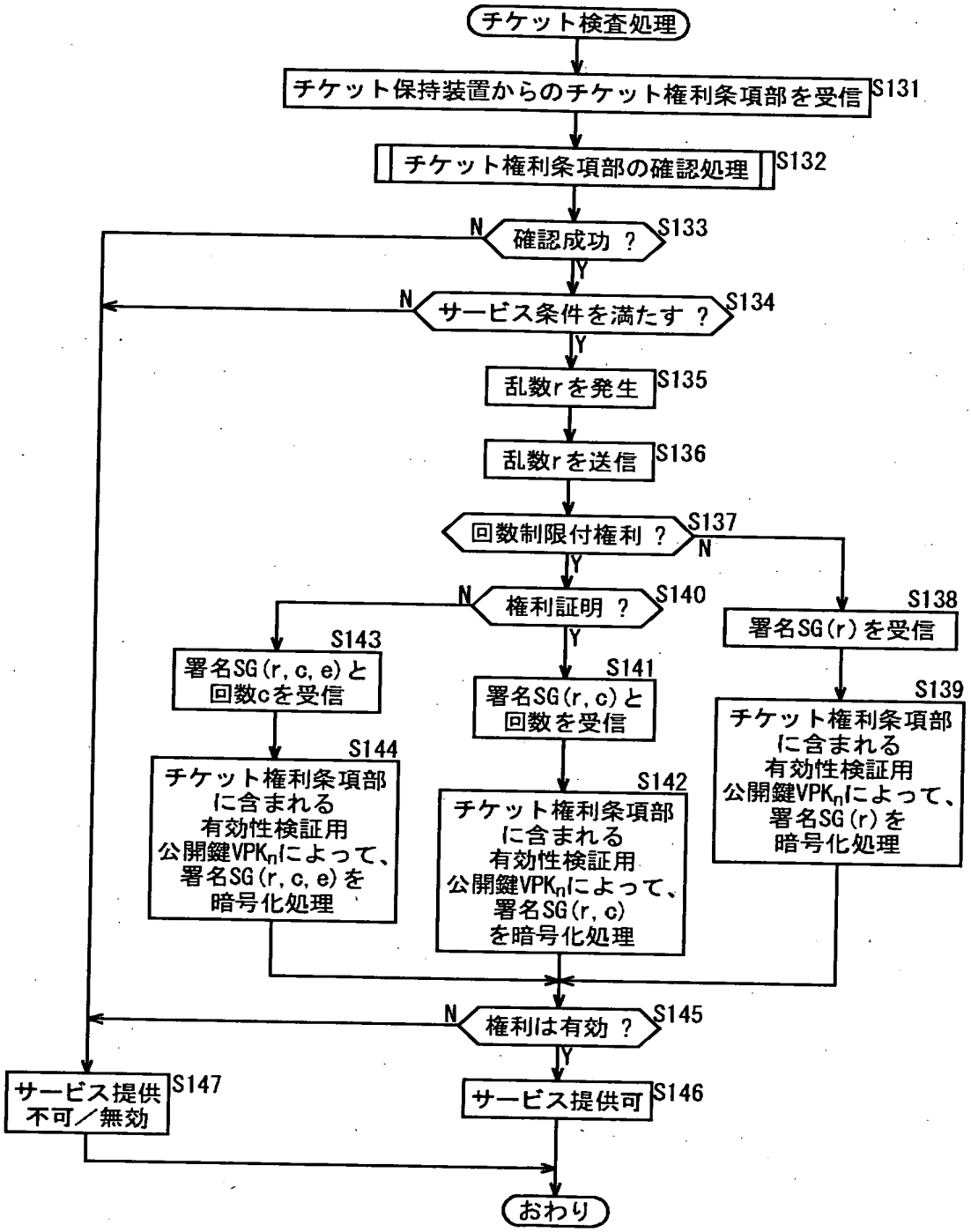
【図１６】


チケットの権利行使/証明処理
行使/証明しようとするチケットのチケット権利条項部を送信
S111
検査側から乱数rを受信
S112
親共通鍵PKで、管理情報を復号
S113
行使/証明対象のチケットのチケット有効性部の復号に用いる子共通鍵CKjを、管理情報から抽出
S114
子共通鍵CKjで、行使/証明対象のチケット有効性部を復号
S115
回数制限付きの権利 ？
S116
Y
N
権利証明 ？
S119
N
Y
行使対象のチケット有効性部の有効性証明用秘密鍵VSKnによって、乱数r、回数c、行使コードeを復号処理することにより、権利証明用署名SG(r,c,e)を生成
S122
証明対象のチケット有効性部の有効性証明用秘密鍵VSKnによって、乱数rと回数cを復号処理することにより、権利証明用署名SG(r,c)を生成
S120
行使/証明対象のチケット有効性部の有効性証明用秘密鍵VSKnによって、乱数rを復号処理することにより、権利証明用署名SG(r)を生成
S117
権利証明用署名SG(r,c,e)と回数cを送信
S123
権利証明用署名SG(r,c)と回数cを送信
S121
権利証明用署名SG(r)を生成
S118
C++
S124
子共通鍵CKjを更新、上書き
S125
新たな子共通鍵CKjによって、チケット有効性部を暗号化、上書き
S126
親共通鍵PKを更新
S127
新たな親共通鍵PKで、管理情報を暗号化
S128
おわり

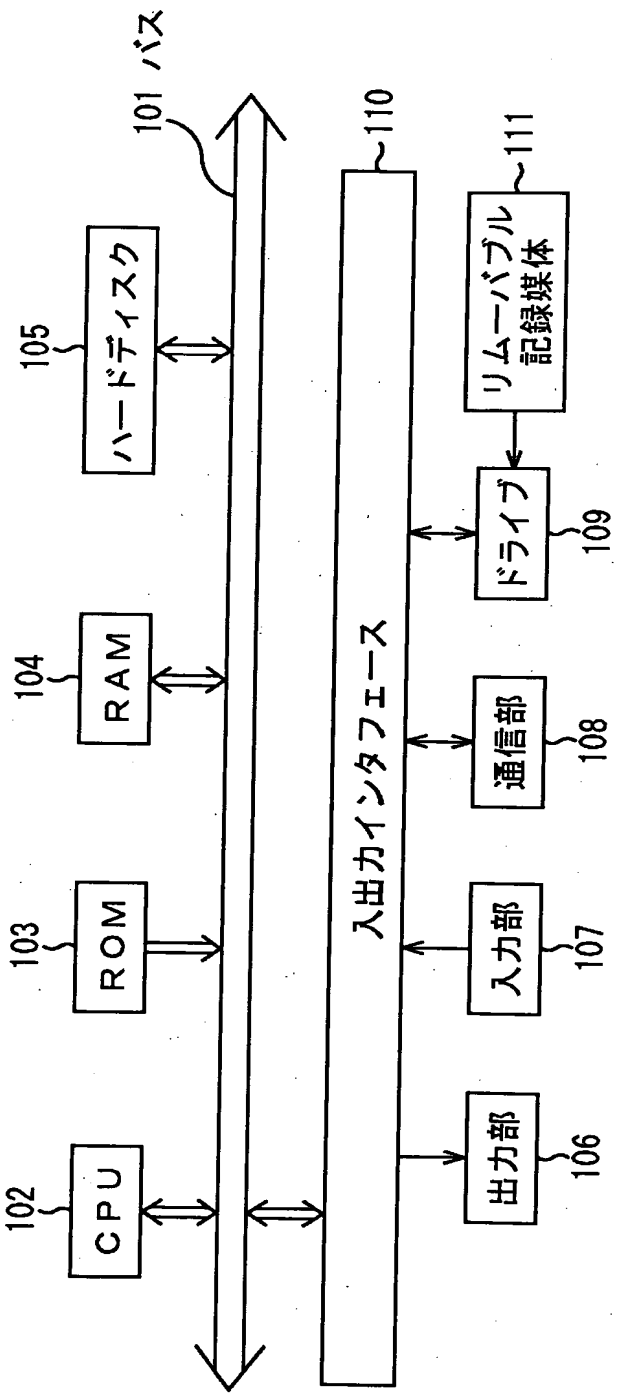
【図１７】


検査内容記憶部
33
表示部
36
乱数発生部
32
31
チケット検査制御部
TPt
署名処理部
34
PCA
署名検証用公開鍵記憶部
35
チケット検査装置 5s
チケット権利条項部等

【図１８】


チケット検査処理
チケット保持装置からのチケット権利条項部を受信
S131
チケット権利条項部の確認処理
S132
確認成功 ？
S133
N
Y
サービス条件を満たす ？
S134
乱数rを発生
S135
乱数rを送信
S136
回数制限付権利 ？
S137
権利証明 ？
S140
署名SG(r)を受信
S138
署名SG(r, c, e)と
回数cを受信
S143
署名SG(r, c)と
回数を受信
S141
チケット権利条項部
に含まれる
有効性検証用
公開鍵VPKnによって、
署名SG(r)を
暗号化処理
S139
チケット権利条項部
に含まれる
有効性検証用
公開鍵VPKnによって、
署名SG(r, c, e)を
暗号化処理
S144
チケット権利条項部
に含まれる
有効性検証用
公開鍵VPKnによって、
署名SG(r, c)
を暗号化処理
S142
権利は有効 ？
S145
サービス提供
不可／無効
S147
サービス提供可
S146
おわり

【図１９】


101 バス
102 CPU
103 ROM
104 RAM
105 ハードディスク
106 出力部
107 入力部
108 通信部
109 ドライブ
110 入出力インタフェース
111 リムーバブル記録媒体
コンピュータ

【書類名】　　要約書

【要約】

【課題】　利便性の高い電子チケットを実現する。

【解決手段】　チケット発行装置３$_t$は、それ自体を外部に示すことなく、その存在を証明することができるアルゴリズムが適用可能な秘密鍵を含む有効性データと、その秘密鍵の存在を検証するのに用いられる、その秘密鍵に対応する公開鍵を含み、有効性データによって、その有効性が証明される被証明情報とを生成し、有効性データと被証明情報とからなる電子チケットを発行する。チケット保持装置４$_u$は、有効性データにおける秘密鍵の存在を証明する電子署名を生成し、被証明情報とともに、チケット検査装置５$_s$に送信する。チケット検査装置５$_s$は、チケット保持装置４$_u$からの電子署名と、被証明情報に含まれる公開鍵とを用いて、チケット保持装置４$_u$における秘密鍵の存否を判定する。

【選択図】　　図１

出証特２００１－３０９９７０２

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社